Inspiring All to Excellence

The Fierté Multi-Academy Trust

Cyber Security Policy

Document and Version Control

Document Title	Trust Cyber Security Policy
Effective Date	October 2021
Policy Owner	Ryan Byrne (*Trust Technical Manager*)
Policy Approver	Trust Board

Version	Date	Amended by	Comments
1.0	10th August 2021	Ryan Byrne	Initial draft for approval by Trust Board.
1.1	~~1~~10th~~7th January~~ May 2023	Ryan Byrne	Reviewed as part of wider Trust IT policy overhaul.

Section	Changes Made
Title	Removed "IT Administration" from policy name.
Throughout	Changes to wording / formatting.
Access Control~~Software Procurement and License Management~~	Added statement regarding SSO and MFA requirements for services.
Network Connectivity	Significant re-write detailing Trust's revised approach.
Technical Support	Added "Technicians' Remit" section.
User Responsibilities	Clarified expectations in line with new Acceptable Use Agreements.

Contents

Introduction

This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any individual and it helps to promote equality across Fierté Multi-Academy Trust.

Key Personnel

Trust Vice-CEO (VC) ~~Tony Hand~~	**Trust Technical Manager** (TTM) ~~Ryan Byrne~~	**Trust Compliance Officer** (CO or DPO)~~)~~ ~~Linda Webster~~
Tony Hand	Ryan Byrne	Linda Webster
Strategic~~, executive-level~~ responsibility for IT across the Trust.	*~~Day-to-day, o~~Operational responsibility for IT across the Trust.*	*~~Acting as the Trust Data Protection Officer, r~~Responsible for Data Protection arrangements and policy ~~in this area~~.*

Commented [RB1]: Reformat this section to provide distinctions between roles and responsibilities.

~~Trust Vice-CEO (*VC*) – Tony Hand~~

~~Trust Technical Manager (*TTM*) – Ryan Byrne~~

~~Data Protection Officer (*DPO*) – Linda Webster~~

Purpose

This document ~~is intended to identif~~defines ~~y~~ standards and expectations ~~which~~ to ~~better~~ protect the Trust ~~data and assets~~ from cyber threats.

Within the context of this document, the term 'users' ~~will~~ may refer to any of the following:

- Full-time, part-time, volunteer and temporary staff employed by, or working for or on behalf of the Trust
- Contractors, consultants and third parties working for or on behalf of the Trust
- All other individuals and parties who have been granted access to the Trust's systems and/or data and information

Ransomware Statement

~~The Trust wish to clearly state that, i~~In alignment with ESFA and NCA guidance, ransoms resulting from cyber-attacks **will ~~not~~ ~~never~~ be paid under any circumstances**.

The Trust acknowledge that, by taking this firm position, the importance of robust preventative measures is increased.

Asset Management

~~Siting of Equipment~~

~~Servers and data storage devices (*including backup tapes and NAS devices*) must be sited in secure, locked areas accessible only to SLT, site staff and technicians. It is unacceptable for such devices to be stored in communal areas or classrooms.~~

Asset Management

Definition

For the purposes of this document, an IT asset is classified as any device which must be configured or managed to achieve security outcomes or which may be impacted as a result of a cyber incident.

Inventory

The Trust maintains a central IT asset inventory. While the TTM is responsible for ensuring accurate records are kept, it is the responsibility of all Trust personnel to ensure they follow processes laid out within this policy before making decisions which may require changes to be made to the inventory.

All IT assets must be labelled with a unique IT asset inventory identifier – in addition to any existing asset tags.

Siting Equipment

Where unencrypted, servers and bulk data storage devices must be stored in secure, locked areas accessible only to SLT, site-staff and technicians. It is unacceptable for such devices to be stored in communal areas or classrooms.

Moving Equipment

From time to time, it may be necessary to re-locate IT equipment in which case the TTM must be informed of the item's 4-digit asset ID as well as the new location's room code. The TTM will then update this information within the asset register.

Donations

Donated equipment can pose a risk to the Trust's IT environment and may fall outside of the standards set out in this document.

Commented [RB2]: Moved this section from under the "Asset Management" heading.

Commented [RB3]: Added clarification regarding the encrypted state of such devices. If data is encrypted at rest, the risk is reduced.

Schools have struggled to find secure spaces where power and data are available. Encrypting data at rest where there is no suitable secure storage location is a suitable compromise.

Donations of IT assets must not be accepted by Academy staff until authorisation has been provided by the TTM or VC. Academies must not allow any equipment to be left on the school premises until such authorisation has been granted.

Donations may be refused for a variety of reasons. For example, they may:

- Cause the Trust to be in breach of policies, legislation or accreditations
- Fall outside of the remit of the Trust Technical Team's expertise
- Require extensive research into or alteration of current device management processes

When a donation is accepted, the donor must be asked to ensure devices have been securely wiped and will be required to submit a 'Donation of IT Asset/s' form (*available digitally via the Policy Portal*). A record of the devices' information (*including manufacturer, model type and serial number*) must then be provided to the TTM by Academy staff for asset-registering.

Procurement

Academies must seek authorisation from the TTM or VC when wishing to procure IT assets to ensure compliance with this policy.

Where a device being purchased may be connected to the internet, it must be well within the vendor's support window. This is to ensure that it will continue to receive security patches into the future.

Presently, Trust's processes support the following end-user operating systems:

Windows 10	iOS	Chrome OS

~~.~~Where a chosen device utilises another operating system, a special exception may be sought from the VC, identifying any additional measures which will need to be put in place before the purchase can go ahead.

The Trust have identified the following minimum specifications for ~~any~~ new devices procured:

Windows Laptops and Desktop~~Trust Vice-CEO (VC)~~		**~~Trust Vice-CEO (VC)~~Multi-Function Devices**	**~~Trust Vice-CEO (VC)~~Networking Equipment**
CPU	i3 (or equivalent)~~Windows 10~~	Must be compatible with PaperCut where printing is likely to be sent from remote devices or high-	Support for: Gigabit switching (with 10GbE uplinks preferred) VLANs
Memory	8Gb DDR4		

Commented [RB4]: Added examples of reasons behind refusing donations. For schools, the refusal of "free" equipment can appear confusing.

Commented [RB5]: Moved to the top of this section as it is sometimes missed by users.

Commented [RB6]: Clarified that this guidance applies to devices being connected to the internet.

Commented [RB7]: Slight reformatting to make for easier reading.

Storage	240Gb Solid State	volume photocopying by multiple users is likely.~~iOS~~	Centralised remote management~~Chrome OS~~
Ports	RJ45 Ethernet USB-C		
Misc.	TPM 2.0		

End of Life Policy and Planning

~~Trust devices~~Devices which ~~are~~ no longer ~~officially~~receive operating system ~~supported by the manufacturer and do not receive~~ security patches ~~are~~ **must not** ~~n~~ be ~~et permitted to~~ connected ~~to~~ Trust networks. This includes ~~. This includes all IT assets such as~~ networking equipment, ~~and~~ photocopiers and ~~as well as~~ end-user device~~s~~s.~~.~~ Where an asset is ~~s are~~ identified as falling into this category, access to the network must be revoked or the device ~~must be~~ replaced.

Where known, the IT asset inventory records device End Of Life (EOL) dates. Academy leaders are informed of these dates by the TTM a~~a~~t the earliest opportunity so that ~~any capital~~ expenditure for replacement devices can be structured into upcoming budgets.~~.~~

When procuring new devices, the Trust will ~~opt~~ adopt ~~for~~ a ~~lease~~ model ~~as this~~in which ~~ensures~~ devices are refreshed at regular intervals ~~while~~ ~~–~~ ~~avoiding~~ minimising large, ~~the need for large, potentially~~ overlooked~~,~~ capital expenditures in future.

~~End of Life Policy~~

~~Trust devices which are no longer officially supported by the manufacturer and do not receive security patches are not permitted to connect to Trust networks. This includes all IT assets such as networking equipment and photocopiers as well as end-user devices. Where assets are identified as falling into this category, access to the network must be revoked or the device must be replaced.~~

Disposal

IT assets must be disposed of in accordance with all relevant legislation including the Data Protection Act 2018 (UK GDPR) ~~UK GDPR~~and the ~~,~~ Waste Electrical and Electronic Equipment Regulations 2013 (WEEE).~~WEEE and other relevant environmental legislation.~~

Commented [RB8]: Clarified that this doesn't apply to an office printer where it will be located next to a user for example.

Commented [RB9]: Concatenated the two separate "End of Life" sections.

Commented [RB10]: Revised wording.

Commented [RB11]: Removed mention of "lease" specifically as this is not always the model used.

Commented [RB12]: Slightly revised wording to more clearly reference legislation.

Where IT assets must be disposed of, Academies must provide the TTM with a register containing the following information:

Device Type	Manufacturer	~~Manufacturer~~Model	IT Asset Number ~~Number~~ *or* Serial Number

~~of manufacturers, models, asset numbers and serial numbers which will then be provided to the TTM.~~ This ~~list~~ will allow disposal to be recorded against the asset inventory and an approved ITAD ~~service~~ provider will be contacted ~~for processing~~by the TTM.

While some legacy assets are likely to be stored ~~around~~ across Academy sites *temporarily*, the Trust ~~will not accept~~does not permit the long-term accumulation of redundant equipment.

Commented [RB13]: Revised for clarity.

Device Configuration

Mobile Device Management

~~To allow for management and visibility, p~~Portable IT devices which are not domain-joined **must** be enrolled into a Mobile Device Management (~~n~~ MDM) platform -wherever practicable.

The Trust has~~ve~~ identified the following MDM platforms ~~into which any of the following devices must be enrolled~~as suitable for the device types listed:

Meraki System Manager~~Multi-Function Devices~~	**~~Networking Equipment~~Google Workspace**	**Microsoft Intune**
iOS and iPadOS *iPhones and iPads*	**Chrome OS** *Chromebooks*	**Windows** *Laptops*
tvOS *Apple TVs*		
macOS *iMacs and MacBooks*		
Android *Tablets and Smartphones*		
Windows *Laptops*		

Endpoint Protection

- ~~iOS (*iPads and iPhones*)~~
- ~~tvOS (*Apple TVs*)~~
- ~~macOS (*iMacs and MacBooks*)~~
- ~~Android (*Various tablets and smartphones*)~~

~~**Google Workspace**~~

- ~~Chrome OS (*Chromebooks*)~~

Endpoint Protection

Sophos Intercept X must be deployed across all Trust-owned Windows and MacOS devices.

Sophos Endpoint policies are defined centrally by the TTM. Wherever possible, settings must be uniform across all devices.

If, due to respective performance impacts and required system capabilities, protection is reduced for any devices, this must be authorised by the TTM or VC. In such a scenario, plans must also be developed to replace the hardware in question as soon as practicable.

As part of the conversion process, before joining the Trust, adequate licenses must be purchased to enrol all academy-convertors' devices into the Trust's Sophos Central tenant.

All endpoint devices must employ the use of a software firewall where possible.

Encryption

All Trust devices with access to personal data must employ at-rest data encryption.

In the case of Windows devices, BitLocker must be enabled on all drives using the onboard TPM for start-up authentication. Where a TPM is not present, a passphrase will be required at device boot. The Trust recognise that this can cause a hinderance to workflow / learning and can impact on ICT lessons in particular. As such, a requirement for TPM has been incorporated into future minimum device specifications. BitLocker recovery keys must be stored in either Active Directory or the Trust's secure IT storage system.

Devices which do not support encryption at-rest should not be connected to any Trust data.

BIOS Protection

Where possible, technicians must ensure a BIOS password is present on devices.

Modification of Managed Settings

Where changes to group policy or device profiles may have a potential impact on cyber security, MSPs and technicians are required to consult with the TTM prior to implementation.

Commented [RB14]: Added comment on academy-convertors. This adds clarity to when this should occur.

Commented [RB15]: Specified "at-rest" data encryption. This clarifies that simply encrypting data while in transit is not acceptable.

Commented [RB16]: Added clarification for learning impact as this has caused issues for lessons in the past.

Commented [RB17]: Added statement covering handling of recovery keys. This has caused issues in the past where a required recovery key could not be found.

Software, Firmware and Operating System Management

Software Procurement and License Management

The Trust maintain a register of all IT-related licenses. Any user wishing to purchase or subscribe to a new software or service must first contact the TTM so that appropriate considerations can be made.

Before raising a purchase order relating to the procurement of new software or licenses, it is the responsibility of the Trust Central Support Team to first ensure the TTM is aware. The TTM will liaise with the DPO to ensure a Data Protection Impact Assessment has been carried out.

A register of all current licenses is held centrally by the TTM. A register of deployed applications / software is included within:

- The Meraki MDM platform for iOS, tvOS, Android and macOS devices
- Google Workspace for Chrome OS devices
- Academy Site Overview documentation for Windows devices

Cross-Trust Alignment

Where possible, cross-Trust alignment of software and operating systems in use minimises the overhead required to manage, patch and update. Reducing variations in software and services used across the Trust also limits the scope of potential attack vectors.

The VC reserves the right to decline the adoption of software and services for which the maintenance overhead may be disproportionate to the benefits provided. Where Trust-approved solutions are available, the VC may instruct Academies to adopt particular software approaches to achieve specified outcomes.
The Trust Board acknowledges that, in some scenarios, this may remove a level of autonomy and increase costs to individual Academies .

Commented [RB18]: General re-wording and structural changes.

Deployment

Deployment

Software deployments are managed centrally at each Academy by technicians. Users ~~are not permitted~~ must not ~~to~~ attempt installation of software onto Trust devices without prior

authorisation from the TTM or VC. Any new deployments must first be approved by the TTM or VC.

Where possible, proportionate technical restrictions should be put in place to prevent the execution or installation of unauthorised applications.

Review of Deployments

During the completion of annual Site Overviews, deployed software will be reviewed with academy leaders. Where software is identified as no longer necessary, technicians will attempt to remotely remove it from devices and will withdraw deployments.

Commented [RB19]: Added clarification that this process will involve SLTs.

Patching and Updates

Trust service providers are expected to ensure security patches are applied within 14 days of release where the addressed vulnerability has been defined as 'critical' or 'high risk' by the vendor. This is monitored by the TTM

.

Commented [RB20]: Removed reference to Technicians' visit reports to reflect changes to IT support structure.

In collaboration with Technicians, the TTM is responsible for ensuring that such patches are deployed internally within this 14-day window.

Where a piece of software no longer receives security patches, it **must** be removed from any networked Trust devices as soon as possible. This is non-negotiable and does not rely on the finding of an alternative product.

Commented [RB21]: Added a strong statement to highlight that only supported software can be used across the Trust.

Backups

Backups form a core-pillar of the Trust's cyber security stance and would prove crucial in ensuring the swift continuation of service after a cyber incident.

A Trust 'Disaster Recovery Policy' has been ratified which explains the strategic approach towards backups in detail.

Networks

Protection

Academies must utilise an onsite firewall appliance to monitor, log and restrict network traffic egress and ingress. Such firewalls must also allow for central, remote management. The Trust's MSPs are responsible for the revising of firewall rules in line with advancing industry standards. Changes may be made to existing rules from time-to-time as the needs of individual Academies require.

Review of Firewall Rules

Review of Firewall Rules

Where the TTM has been provided access to manage firewall rules, any exceptions will be reviewed at least annually to ensure they remain suitably restricted in scope.

Network Connectivity

Only Trust-managed devices may ever be physically connected (*i.e. via ethernet*) to Trust networks.

Users are not permitted to connect their own networking equipment to Trust infrastructure as doing so could increase the risk of intrusion.

Where devices connect to Academy infrastructure via wireless networks, the configuration must be secured using WPA2 security at a minimum.

The Trust recognise that, across most academies, both BYOD and Trust devices occupy the same wireless networks. Academy staff are also currently able to grant access to wireless networks for guests.
A lack of network segmentation can pose a risk and, as such, a long-term plan is under development. The below describes the Trust's policy as it is to be implemented.

Each academy must broadcast the following wireless networks at a minimum:

Each academy must broadcast the following wireless networks at a minimum:

Each academy must broadcast the following wireless networks at a minimum:

Each academy must broadcast the following wireless networks at a minimum:

"Trust"	"Guest"	"IoT"
Intended only for Trust-owned devices.	*Intended for BYOD devices.*	*Intended for Internet of Things (IoT) devices.*

Allows for access to Trust resources and the internet.	Separate VLAN to segregate all network traffic. Allows for limited web access only. No access to Trust resources such as servers of photocopiers.	Separate VLAN to segregate all network traffic.
Only the TTM and Technicians are aware of the PSK	*Headteacher are provided with the PSK and have authority to grant users access as required.*	*Only the TTM and Technicians are aware of the PSK.*

Where an external user is granted access to ~~the~~a network, the individual providing access ~~is expected~~ must ~~to inform the end-user of any relevant IT and~~ ensure the ~~a~~relevant Acceptable ~~u~~Use ~~p~~Policy has been shared~~ies.~~ In some instances, ~~The end-user is also to be informed that their network activity will be logged by the Academy's ISP. It may be necessary for~~ the end-user may need to install a Certificate Authority~~A~~ which will allow for encrypted traffic to be intercepted and logged by the- Trust. This is available from the Trust Technical Team upon request~~ISP.~~

Commented [RB22]: Significant re-write to detail the *work-in-progress* ideal approach to connectivity.

~~Users are not permitted to connect their own networking equipment to Trust infrastructure as doing so could increase the risk of intrusion.~~

~~Only the TTM, VC and cross-Trust technicians are permitted to hold network credentials for any central Trust SSIDs.~~

~~Only Trust-managed devices should ever be physically connected to any Academy's network.~~

Technical Support

Procurement and SLAs

Any ~~T~~Technical Support SLA~~s~~ must be approved by the TTM or VC before acceptance / renewal. ~~Due to the key role they play, t~~The Trust reserves ~~-~~the right to specify which service providers can or cannot be used by a~~A~~cademies.

Direction of Technicians and External Support

The TTM is responsible for the line management and day-to-day direction of Technicians in alignment with current Trust priorities. ~~The TTM~~ Similarly, the TTM and VC reserve ~~s~~ the right to direct the priorities of any external IT support agencies ~~in line with current Trust priorities~~.

Commented [RB23]: Revised wording to better represent new IT support structure.

~~-~~For example, while an ~~A~~academy leader may wish for a technician's visit or support agency's time to be spent resolving a particular issue, in some instances it may be necessary for another ~~action~~ task to be prioritised such as the deployment of an urgent patch.

Technicians must seek approval from the TTM before making any changes to visit arrangements. Wherever practicable, the TTM must consult with academy leaders to ensure such arrangements remain convenient.

Any technician working onsite at an academy is to be provided with a licence to access to the Trust's central password manager for that site.

Technicians' Remit

User's support requests *may* impact on the cyber security stance of the Trust or bring into question the Trust's compliance with policies, legislation or accreditations. In such scenarios, Trust Technicians are not authorised to proceed without first seeking clarification from the TTM. Wherever practicable, users should be kept informed of the process being followed and status of the request.

In some instances, the TTM will also need to escalate and consult with the VC as Trust Strategic IT Lead.

~~Windows Laptops and Desktop~~	~~Multi-Function Devices~~	~~Networking Equipment~~
~~CPU~~ ~~i3 (or equivalent)~~	~~Must be compatible with PaperCut where printing is likely to be sent from remote devices or high volume photocopying by multiple users is likely.~~	~~Support for:~~ ~~Gigabit switching (with 10GbE uplinks preferred)~~ ~~VLANs~~ ~~Centralised remote management~~

Visit Reports

Visit Reports

Where an external technician visits academies on a rota, they are expected to complete a visit report briefly detailing key information such as the success of backups and status of updates / deployments. These reports must be provided to the TTM by the end of the working day to allow for timely review and actioning of any concerns identified.

Commented [RB24]: Inserted this statement to highlights that consent of academies remains important in this.

Commented [RB25]: Added section which highlights that technicians and I may need to carefully consider actions and implications on Cyber Security.
I feel it is important to define this current practice in policy.

Commented [RB26]: Clarified that this doesn't apply to an office printer where it will be located next to a user for example.

Commented [RB26]: Clarified that this doesn't apply to an office printer where it will be located next to a user for example.

Trust Personnel

New Starters and Leavers

For all Academy-specific staff / volunteers, it is the responsibility of the Headteacher to inform the TTM via the Support Portal within 10 working days of a leaver / new starter. For OPOJ staff / volunteers, this same responsibility lies with the OPOJ Regional Manager.

For all Academy-specific staff / volunteers, it is the responsibility of the Headteacher to inform the TTM via the Support Portal within 10 working days of a leaver / new starter. For OPOJ staff / volunteers, this same responsibility lies with the OPOJ Regional Manager.

Securing Accounts

In addition to the guidance set out in the Trust's Password Policy, users **must** lock / secure devices when not in use. For example, if a class teacher steps out of the classroom to collect printing – however briefly – the desktop which they were working at must be locked. On a Windows device, this can be achieved by pressing the "Control", "Alt" and "Delete" keys simultaneously and then selecting "Lock".

Education and Training

Upon induction, all new users will be required to complete cyber security awareness training. This package will be reviewed by the TTM at regular intervals to ensure it addresses issues relevant to the current IT landscape.

Users are required to complete similar annual refresher training for which Academy leaders must report attendance to the TTM.

Assistance

In some circumstances, a technician / the TTM may instruct users to take specific action to ensure necessary updates are applied in a timely manner. In such cases, there is an expectation that users will comply with these requests or inform the technician / TTM at the earliest opportunity if this is not possible.

Responsibility to Report

Where users are aware of non-compliance with this policy, the Trust recommend that they raise this in a professional manner. The Support Portal can also be used to submit anonymous reports by choosing "no" when asked if able to access Office 365.

In the event of a suspected cyber security incident, all users are required to contact the TTM immediately. If the TTM is unavailable, the VC must be contacted.

The TTM will then work alongside industry partners to establish a course of action and will attempt to preserve any evidence. Depending upon the severity, it may be necessary for resources from the Trust's Cyber Insurance provider to become involved.

Where an incident occurs that causes another person or organisation to suffer, there could be serious implications should it be deemed that the Trust did not take appropriate and timely action.

Disciplinary Action

Failure to comply with this policy may result in disciplinary action up to and including dismissal.

Risk Management

Site Overviews

The TTM visits each Academy (*at least*) annually to update a Site Overview document. These Site Overviews are intended to provide technicians, leaders, the VC and the Trust Board with a brief outline of the IT environment within each Academy.

Risk Register

A risk register is maintained across each Academy by the TTM. This is updated (*at least*) annually in line with the Site Overviews and is shared with the VC and Trustees.

Resourcing

The Trust recognise that IT now forms a crucial pillar not only in regards the delivery of the curriculum and data protection but also the safeguarding of the Trust's reputation.

Sufficient resources should be made available centrally as well as within individual Academy budgets to comply fully with our legal obligations and to ensure compliance with Trust policy. Where a risk is recognised as emerging due to a lack of resourcing either at a Trust or an Academy level, the TTM will identify this in writing to the VC.

Response Testing and Practice

The TTM and VC utilise industry tools (*such as the NCSC's exercise in a box*) to evaluate the Trust's response to hypothetical cyber incidents at least annually. Where additional considerations are highlighted during these exercises, policies and procedures are adapted accordingly.

Annual Audits

The Trust appoint an external organisation to undertake annual Cyber Security audits. The outcomes of these audits are provided to the Trust Board – identifying areas of strength as well as areas which need further improvement. Each audit will provide recommended actions categorised based upon their urgency as well as an overall level of assurance for the Trust.

~~As of the writing of this policy, the most recent internal Cyber Security audit was conducted **in August 2021**. The next audit is due to take place in the **summer term of 2022**.~~

Access Control

Access to systems and data will be controlled and limited following the principle of 'least privilege'.

Trust Technical Manager

The TTM must be provided with an account allowing for (*at minimum*) user account management across any services and administrative systems in use within the Trust.

Dedicated Administrative Accounts

Wherever practicable, users who require administrative access will be provided with a dedicated account separated from their standard account. Approaching access in this way reduces the risk should a user's primary account become compromised.

Wherever practicable, MSPs and external support agencies will be provided with dedicated accounts to execute their roles and perform any necessary functions – allowing for a more precise audit trail of admin activities.

Review of User Accounts

At least annually, the TTM will provide Academy leaders with an inventory of active user accounts across all known systems and services. Leaders will be expected to review and return the documents within 14 days – identifying any accounts that are no longer needed or that may no longer require the same level of access.

User Responsibilities

Amongst others, the Trust has produced the following concise Acceptable Use Agreements:

EYFS and KS1 Class Agreement	**KS2 Class Agreement**	**Learner Agreement**
Provided Device Agreement	**Staff, Agency Worker and Volunteer Agreement**	**Visitor Agreement**

Users of Trust systems and/or networks must do so in accordance with these.

The Trust expect that:

- Class agreements are discussed with learners during the transition period or at the start of each new academic year.
- Parents / carers review and sign the learner agreement on behalf of their child/ren.
- Academy Senior Leadership Teams and office staff ensure any visitors, staff, agency workers or volunteers sign the appropriate agreement **before** being granted access to Trust IT facilities.
- Where a Trust device has been provided for use by an individual, the "provided device agreement" is signed **before** access is granted.

Privilege Management

Users are not permitted to have admin-level privileges for local devices except for extraneous circumstances where this is deemed necessary by the TTM. In such an instance, this can only be allowed where LAPS is active on the device.

MSPs, technicians, the VC and TTM are the only parties permitted to utilise accounts possessing domain or global admin-level privileges. However, it is down to the TTM's discretion as to which MSPs / technicians receive this level of access to individual systems and services. In some scenarios, limited privileges may be granted to non-IT users where this has been agreed in writing with the VC or Academy leaders – for example, password-reset capabilities may be granted to a specific member of the SLT for users at their site.

Remote Access

The Trust's choice of remote access software must be deployed to any compatible Trust devices. Use of remote access software is logged and Trust technicians are not permitted to remotely access a user's device without first seeking authorisation from the user or a member of the Academy's / Trust's leadership team. In extreme circumstances, where it may be necessary to deviate from this procedure, the VC will be informed and a log kept.

Single Sign On and Multi-Factor Authentication

Where a service or platform lacks Multi-Factor Authentication (MFA) or Azure AD Single-Sign-On (SSO) capabilities, the Trust will look to identify a suitable replacement. This is a significant requirement and may result in the ceasing or non-renewal of SLAs.

Glossary

- NAS (Network Attached Storage)
    - A device which stores data accessible over the local network. The Trust Disaster Recovery policy requires the use of a NAS device to which server data is then backed-up.
- MDM (Mobile Device Management)
    - A cloud-hosted platform to which devices report their status and receive their configuration.
- Domain (Active Directory Domain)
    - A group of objects (*computers and users*) which share settings that are managed in a central location.
- Group Policy
    - Settings which are defined centrally by an administrator for a subset of users / devices.
- ISP (Internet Service Provider)
- CA (Certificate Authority)
    - A trusted organisation or entity which provides third-party authentication of digital cryptographic certificates presented by a service or website.
- SSIDs (Service Set Identifier)
    - The primary name broadcast by a wireless network.
- MSPs (Managed Service Providers)
    - An external organisation commissioned to provide specific IT services to the Trust / Academy.
- LAPS (Local Admin Password Solution)
    - A Microsoft product which automatically rotates local admin passwords on individual domain devices – writing the credentials back to Active Directory.