CONSILIUM ACADEMIES

IT Security

Policy

2023/2024

PARTNERSHIPS | OPPORTUNITY | INTEGRITY | EQUITY | EXCELLENCE | PEOPLE-CENTRED

Date of Approval:	April 2023
Approved by:	Trust Board
Date of next Review:	September 2024

Consilium Academies

Enriching Lives, Inspiring Ambitions

Introduction

The Trust has a statutory duty to keep children safe whilst receiving education through its schools. This is set out in the government's guidance 'Keeping Children Safe in Education'.

This duty extends to both on-site and remote learning. These ICT regulations therefore set out the minimum standards required of the Trust's ICT environment to enable safe learning in line with KCSiE whether on school sites or through remote provision.

This document is approved annually by the Board of Directors and applies to the Trust, all its Schools and, if applicable, its subsidiary undertakings.

Compliance with these regulations is compulsory for all staff connected with the Trust and its Schools. A member of staff who fails to comply with these Regulations may be subject to disciplinary action under the Trust's disciplinary policy and the Board of Directors will be notified of any such breach. It is the responsibility of individual school Senior Leadership Teams (SLT) and Local Academy Boards (LAB) to ensure that staff are made aware of the existence and content of the Trust's ICT Regulations.

In exceptional circumstances, the Head of Technical Services may authorise a departure from the detailed provisions of these regulations. In such circumstances, the Chief Finance and Operating Officer will maintain an appropriately detailed dispensation register to formally record such decisions.

These regulations should be read in conjunction with other relevant Trust policies, in particular the Data Protection Policy, Safeguarding and Acceptable Use Policies.

Roles and Responsibilities

The responsibility for keeping children safe in education extends to all employees and Directors of the Trust. The following, however, sets out the specific aspects of those responsibilities relating to the ICT control environment.
The Trustees are responsible for approving a set of ICT regulations which meet the statutory duties set out in government guidance and regulation; and monitoring Trust-wide compliance with the defined ICT regulations.

The Head of Technical Services is responsible for:

- establishing a set of ICT regulations which meet the statutory duties set out in government guidance and regulation;
- Obtaining assurance around the compliance with the defined regulations and reporting routinely to the Board of Directors.

The Data Protection Officer (DPO) is responsible for:

- Informing and advising the Trust and its employees of their obligations under the General Data Protection Regulations (GDPR) and other data protection related legislation;
- Supporting the DFO in the establishment of these regulations in relation to data;
- Monitoring compliance with the Trust's data protection related policies; and
- Providing advice in relation to Data Protection Impact Assessments.

Local Academy Boards are responsible for:

- Receiving assurance that all school staff and visitors are made aware of the existence and content of the Trust ICT regulations;
- Monitoring compliance with the defined ICT regulations for their school;
- Operations around the school's approach to meeting the requirements of and ensuring compliance with the ICT regulations.

Headteachers are responsible for:

- Communicating the existence and content of the ICT regulations to all staff, and visitors, and providing this assurance

to the LAB;
- Identifying and addressing any instances of non-compliance with the Head of Technical Services.
- Providing the LAB, DFO or Trustees with necessary data or information to provide assurance over the systems of control implemented and the compliance with those controls.

Internal auditors will be engaged by the Trustees to routinely monitor compliance with regulations and provide recommendations to improve and/or strengthen the overall ICT control environment. The internal auditors will provide independent and objective assurance on the adequacy and effectiveness of design and implementation of the systems of internal control.

Other roles and responsibilities. Should any other specific role or responsibility with respect to the ICT control environment not be clearly defined above, the Head of Technical Services should be consulted to determine the most appropriate group to perform the role.

Access Controls

A fundamental requirement underpinning these ICT regulations is that users of the ICT systems are individually identifiable, and that activity undertaken by each individual can be tracked. It is therefore essential that each individual users' access to systems is appropriately secured.

Shared accounts should be avoided. Where several users require access to a single mailbox for instance, this can be achieved through shared access from individual accounts rather than a shared account. Any instances of shared accounts must be reported to and authorised by the Head of Technical Services, and wherever possible be replaced with shared access through individual accounts.

The Trust must be assured that schools' ICT systems include appropriate security arrangements to prevent unauthorised access to individual staff and Trustee accounts.

Strong passwords are required for all staff. This must be a sufficiently long and complex combination of letters, numbers, and special characters.

To facilitate ease of use and accessibility, students' accounts may require less stringent password and multi- factor authentication requirements. Schools, in conjunction with the Head of Technical Services guidance, will implement access controls on students' accounts that they deem appropriate.

Two factor authentication must be in place for all systems utilised by staff and students that can be remotely accessed. This includes third party cloud hosted systems.

Wherever possible, schools should procure software that integrates with the Trust Microsoft 365 platform for secure access and single sign on.

Only IT support staff will hold the Trust wide Wireless encryption password. This must not be shared with any staff including leadership post holders. Instead, an isolated guest (BYOD) network will be provided and can be freely shared.

Staff will have restricted access to the network that grants them the most limited set of permissions needed for their role, reducing the risk of a security breach by preventing accidental contamination.

No staff member will hold administrator permissions unless approved by the Head of Technical Services. Generally, these rights will only be held by IT support staff. The Head of Technical Services will hold a register of all approved administrators and their access levels.

The domain administrator account will only be used when necessary. It will be secured with a complex password that is changed each year. Only the Head of Technical Services and the Technical Delivery Manager will have a copy of this credential.

Cluster Network Managers and central IT support staff will have Domain Administrator accounts where this is required. These

accounts will be separate to their standard staff logon and only used when necessary for troubleshooting or configuration tasks. The passwords on these accounts will change every 90 days and must be complex.

IT Engineers will receive local administrator rights via a secondary account. These accounts will have restricted access to their school only and the key systems that they must administer. IT Engineers will not have access to other schools or centrally managed infrastructure.

Any services or applications that require a user account to be run should not use an engineer or the domain administrator account. A separate service account should be created and used with the details being recorded in the site/Trust documentation.

Security Baseline

All infrastructure is protected with secure, complex passwords. These are changed on a regular basis, and the top-level 'full access' accounts are only used when required.

The default passwords for all devices are changed before they are allowed onto the secure network.

Only devices that are joined to the appropriate device management system may access the Trust secure network – e.g. Active Directory, Microsoft Endpoint Configuration Manager, Apple School Manager, Google Tenant
Security updates are applied to all network devices on a fortnightly basis.

Only devices that are running a supported operating system with appropriate support and security patches are allowed on the network.

Applications that are not no longer updated or supported by their developer must not be used.

Unmanaged (i.e. devices not owned and configured by the Trust) will be treated as unsecured devices and will not allowed onto the Trust network.

Spam filtering is applied to the school email system to reduce the likelihood of phishing emails being received by the end user.

The Trust network will not allow users, including staff and leadership, to download or install any software. Only the IT team can undertake this function, preventing users from downloading software that appears legitimate but can track usage or cause reliability and security concerns.

A remote access solution is available that allows staff to work on files from home. Users are not permitted to download files or transfer any files onto the network. The remote access solution only authorises connection to a specific part of the network.
All schools in the Trust will use a Sophos XG firewall to manage their network perimeter security.

All firewalls must operate with a 'deny' all approach – changes to the allowed firewall rules must be documented and approved by the Technical Delivery Manager or Head of Technical Services.

All staff and students are given access to the most up-to-date version of Microsoft 365 software.

Servers and critical infrastructure are updated with the latest patches monthly. Exceptions to this are limited and made only when absolutely required.

Network infrastructure devices have their firmware updated on an annual basis, or as required in the event of a critical update/compatibility issue arising.

Each school will have appropriate hardware to backup it's data. This will vary from tape loader to a SANor NAS box. Physical and logical access to this media is restricted to protect the files from attack. All data will be encrypted by the backup software. All schools will have a cloud backup solution that hosts an off-site copy of their server infrastructure in a UK based datacentre. Data will be encrypted during transit and whilst at rest.

Schools will utilise the Office 365 to store their critical data. There will be no on-premises file storage for staff and student data

allowed unless otherwise agreed with the Head of Technical Services.

The Technical Services team will audit each school every 12 months. A full security review will be carried out for each device. Any device that does not meet the current standards will be immediately decommissioned.

Bitlocker encryption will be automatically enforced on any device that meets the minimum specifications.

Limited use of pen-drives is only permissible where BitLocker encryption is enabled. All other encryption technologies are not supported.

Office 365 Rights Management Protection is used to provide a secure and encrypted e-mail facility.

All devices will automatically 'time out' and lock after a period of inactivity. For curriculum devices, the timeout will be 60 minutes. For central and office based administrative staff, the timeout will be 20 minutes.

All staff must undertake annual Cyber Security Awareness Training from the NCSC. Staff are given advice and guidance on the proper use of the school network to reduce the risk of contamination.

Staff are aware that they can, and feel confident to, speak with the Technical Services Team if they are unsure of anything. Staff receive advice and information from Technical Services during periods of high cyber-security threat.

Data users MUST ensure that they do not allow individuals who are not directly employed by the Trust access to the Trust's electronic devices.

Devices MUST be locked or logged off when left unattended.

The use of personal cloud storage systems (e.g. personal Dropbox, iCloud, Google Drive etc) is strictly prohibited. Staff and students must only use the Trust managed cloud storage solutions.

Staff are supported with the correct use of their home computers, and where possible are assisted to ensure they make informed and secure decisions to reduce the risk to the school's/Trust's network.

Disclaimers are automatically added to incoming mail to continually remind users of the risk from phishing e-mails.
Automated user management software is utilised to create and remove user accounts as required. Technical Services, along with HR and BSOs, will conduct a manual audit of the user accounts each term.

Any breaches of the IT security guidelines must be reported immediately to the Head of Technical Services.

All compatible devices must be protected with the Trust's chosen anti-virus and ransomware protection
– tamper protection must always be enabled.

Best practice must be followed in the configuration of the security systems – any deviation from this must be agreed in advance with the Head of Technical Services.

Appropriate Filtering

The Trust is required to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering.

The Trust is expected to assess the risk of our children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology.

The Trust is obliged to ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the schools' IT systems.

However, schools need to be careful that "over blocking" does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

The Trust must be assured that systems ensure that access to illegal content is blocked, specifically that filtering providers:

- are Internet Watch Foundation (IWF) members and block access to illegal Child Sexual Abuse Material (CSAM); and
- integrate the 'police assessed list of unlawful terrorist content, produced on behalf of the Home Office'.

Recognising that no filter can guarantee to be 100% effective, the Trust must be assured that filtering systems manage the following content:

- Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of protected characteristics listed in the Equality Act 2010.
- Drugs / Substance abuse: displays or promotes the illegal use of drugs or substances.
- Extremism: promotes terrorism and terrorist ideologies, violence or intolerance.
- Malware / Hacking: promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content.
- Pornography: displays sexual acts or explicit images.
- Piracy and copyright theft: includes illegal provision of copyrighted material.
- Self-Harm: promotes or displays deliberate self-harm (including suicide and eating disorders)
- Violence: displays or promotes the use of physical force intended to hurt or kill.

The above list should not be considered exhaustive.

The Trust must be assured that schools' filtering systems meet the following principles:

Age appropriate / differentiated filtering includes the ability to vary filtering strength appropriate to age and role.

- Circumvention: the ability to identify and manage technologies and techniques used to circumvent the system, for example VPN, proxy services, and DNS over HTTPS.
- Control: the ability and ease of use that allows schools to control the filter to permit or deny any specific content.
- Filtering Policy: a published rationale that details the approach to filtering with classification and categorisation as well as over blocking. A clearly differentiated level between staff and pupils should be defined.
- Group / Multi-site Management: the ability to deploy central policy and obtain central oversight.
- Identification: the system can identify specific users.
- Mobile and App content: the system is effective in blocking inappropriate content via mobile and app technologies.
- Multiple Language Support: the ability for the system to manage relevant languages.
- Network Level: wherever possible, filtering is applied at the network level rather than being reliant on software on user devices.
- Reporting Mechanism: the ability to report inappropriate content for access or blocking.
- Reports: the system offers clear historical information on the websites visited by users and the preventative measure taken where applicable (i.e. sites blocked)

Remote Learning

There are occasions where a school may choose to provide a device for students to utilise at home to support their learning. The device will always remain property of the Trust. Parents and carers may be held liable for any damage to the device.

The Trust will provide appropriate safeguarding and security software for the device. Schools must not allow a device to leave the school premises until a member of the Technical Services team has confirmed the appropriate safeguards are in place.

The school must keep appropriately detailed records of the devices it has assigned for home learning – at a minimum this must include the device make, model, serial number or asset tag, and the name of the student receiving the device.

The school safeguarding team is responsible for monitoring usage on the device.

The device must be used in accordance with the school's acceptable usage policy at all times.

The device must be used for school-based learning only. Personal use is not allowed.

All usage of the device is monitored. Any inappropriate usage will result in the device being remotely disabled.