Cyber & Technical Security Policy

Date Prepared	March 2026
Author	Sarah Jones and Kerry Jordan-Daus
Scrutinised by (Trustee)	Gavin Sibbick
Date ratified	31 March 2026
Review date	March 2028

Aims and Introduction

Ensuring the security of our technology is critical to keeping our children safe and to the delivery of high-quality education. The Cyber & Technical Security Policy sets out Veritas Multi Academy Trust's commitment to practice achieving these aims. This depends not only on technical measures, but also on good user professional development and education.

The Trust utilises a number of policies to deliver on the core aim including Safeguarding, People Development, Induction, Staff Code of Conduct, Acceptable Use agreements, the Data Protection Policy and our Risk and Audit Policy.

The Cyber & Technical Security Policy ensures that the Trust fulfils its responsibilities to comply with Keeping Children Safe in Education and with the Risk Protection Arrangement (RPA).

Responsibilities

We all have a responsibility to ensuring technical security. To this end the Trust is committed to a robust professional development for all our people and a comprehensive education programme for our children.

Specific responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff.

The strategic management of technical security will be the responsibility of the Trust Business Manager, the operational delivery of key services will be delivered by the Trust's technology provider. Headteachers and Designated Safeguarding Leads additionally have key responsibilities.

The Trust's Risk and Audit Committee and the Trust's central risk register will record incidents, maintain oversight of mitigation and report to the Trust Board on all matters pertaining to technical security.

The Trust has Risk Protection Cover (Risk Protection Arrangement :RPA) which includes cover for Cyber Incidents, defined as

"Any actual or suspected unauthorised access to any computer, other computing and electronic equipment linked to computer hardware, electronic data processing equipment, microchips or computer installation that processes, stores, transmits, retrieves or receives data." (RPA)

RPA cover includes a 24/7 dedicated helpline and dedicated email address. In the event of a Cyber Incident the contact is RPA Emergency Assistance Helpline.

To meet the criteria for RPA, the Trust has in place the following as agreed with the Technology Provider

1. Have in place a Cyber Response Plan (See Cyber Disaster Plan)

2. Have a backup process (See Cyber Disaster Plan)

3. All Employees, Trustees and Governors undertake Cyber Security Training. This is annually updated and forms part of our Induction for new staff, trustees and governors.

4. The Trust is registered with Police CyberAlarm.

Infrastructure and Systems

- The Trust's technology is managed in accordance with best practice and compliant with recommendations to ensure secure and safe use.
- The Trusts technology provider will undertake regular reviews and audits of the safety and security of the Trust's technical systems to ensure compliance.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the Trust systems and data. This includes Multi Factor Authentication being in place for the Trust Central team and other users where access is appropriate.
- The Trust's technology provider is responsible for the filtering system and reporting issues associated with breaches.
- Servers, wireless systems and cabling must be securely located and physical access restricted.

- The Trusts technology provider is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- The Trust's infrastructure and individual devices are protected by up-to-date software to protect against malicious threats from cyber-attacks.

Users

- The Trust ensures that all users, through induction, professional development and ongoing professional development, understand their responsibilities for technical security
- The Trust's Acceptable Use for all staff and children and for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the Trust system clearly sets out responsibilities
- All users will have clearly defined access rights to the Trust's technical systems.
- Details of the access rights available to groups of users will be recorded by the Trusts technology provider and will be reviewed, at least annually, by the Trust Business Manager.

USB's and Portable Devices

- Users should reduce the use of USBs/portable devices where possible, using cloud storage solutions, ie. SharePoint, for sharing and storing data whenever possible.
- USB's/Portable devices shall not be used to store sensitive or personal data at any time.
- All users must only use school-approved encrypted USB sticks/portable devices.
- Users must report any lost or stolen USB sticks/portable devices immediately to the School Data Protection Officer who will record this and investigate whether, depending on the nature of data held on the device, is to be reported to the ICO. The Trust DPO to be advised of the breach (via Governance Professional).
- USB sticks/portable devices used must be scanned for viruses and malware.

Password Security

All users have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security. Children will be taught this as part of their education programme.

Adult passwords:

- Members of staff and other adults will be made aware of the Trust's password policy:
- All Trust networks and systems are protected by secure passwords.
- Passwords are set to ensure security. Passwords should be easy to remember, but difficult to guess or crack.
- All users have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of the Trust.
- Requests for password changes are carried out through our technology provider where trained staff will take steps to ensure the authenticity of the user making contact.
- Multi Factor Authentication is in place for the Trust Central team and other users where access is appropriate to further secure access.

Learner passwords:

- Records of learner usernames and passwords are kept in an electronic form and are secure when not required by the user. These are managed by class teachers.
- Learners are taught the importance of password security, and includes how passwords are compromised, and why these password rules are important.

Filtering

In accordance with Keeping Children Safe in Education and our Trust's Safeguarding and Child Protection Policy, the Trust has in place a robust filtering system. Our Trust's professional development for all adults and our education programme for all learners makes explicit the purpose of filtering. Parents will be informed of the Trust's filtering policy through the Acceptable Use Policy, through online safety awareness newsletters and our ongoing communications with families.

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed.

Everyone has a responsibility to raise a concern if inappropriate content can be accessed. All users have a responsibility to report immediately to the Designated Safeguarding of the Trust's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering/security systems in place to prevent access to such materials. No amendments to filtering will be applied without prior approval of the Headteacher for education related or the Trust Business Manager for business. Where personal mobile devices are allowed internet access through the Trust network, filtering will be applied that is consistent with Trust practice.

- Internet access is filtered for all users.

- Differentiated internet access is available for adults and customised filtering changes are managed by the Trust.
- Filter content lists are regularly updated, and internet use is logged and monitored.
- The monitoring process alerts the Trust to breaches of the filtering policy, which are then acted upon.
- Mobile devices that access the Trust internet connection (whether Trust or personal devices) will be subject to the same filtering standards as other devices on the Trust systems

Monitoring

Robust systems are in place to monitor the Trust's technical security and the implementation of this policy. This includes day-to-day monitoring and periodic external audits as part of the Trust's Risk and Audit Policy. All individuals have a monitoring responsibility. The Trust Business Manager has a strategic responsibility for ensuring through monitoring the robustness of our policies and practices.

Our monitoring includes:

- Ensuring through induction, professional development and the education programme that all users are aware of this Policy
- Headteachers and the Trust Business Manager ensure that all users are aware that use of Trust network and computing resource is monitored by the Trusts technology provider.
- An appropriate system is in place for users to report any actual/potential technical incident to the Designated Safeguarding Lead
- The Trust's technology provider will undertake regular reviews and audits of the safety and security of the Trust's technical systems and provide reports to the Trust Business Manager and Head Teachers
- Logs of filtering change controls and of filtering incidents will be made available to External Filtering Provider/Local Authority/Police on request. Logs are held for 365 days.

Preparation and Additional Resources

The following Checklist is annually reviewed as part of the ongoing compliance and safety programme. This will be reported to the Trust Risk and Audit Committee.

Checklist	Completed
• Regularly review Cyber & Technical Security Policy	
• Assess the Trust/Schools current security measures against Cyber Essentials requirements, such as firewall rules, malware protection, and role based user access. Cyber Essentials is a government-backed baseline standard, which we would encourage all RPA members to strive towards achieving wherever possible.	
• Ensure Multi-Factor Authentication (MFA) is in place: A method of confirming a user's identity by using a combination of two or more different factors.	
• Implement a regular patching regime: Routinely install security and system updates and a regular patching regime to ensure any internet-facing device is not susceptible to an exploit. This includes Exchange servers, web servers, SQL servers, VPN devices and Firewall devices. Ensure that security patches are checked for and applied on a regular basis. Vulnerabilities within Microsoft Exchange Servers have been the root cause of many cyber-attacks in the past. It is highly recommended that on-premises exchange servers are reviewed and patched/updated as a high priority and moving to an Office 365 environment with MFA if possible.	

• Enable and review Remote Device Protocols (RDP) access policies: The use of external RDP access to a device is not recommended and allows attackers to brute-force access to any device that is externally accessible. Mitigating measures are: o If external RDP connections are used, MFA should be used o Restricting access via the firewall to RDP enabled machines to allow only those who are allowed to connect o Enable an account lockout policy for failed attempts o The use of a VPN tunnel to access a network in the first instance, and then allowing users to subsequently use RDP or RDS to access a device afterwards is highly recommended	
• Review NCSC advice regarding measures for IT teams to implement: Mitigating malware and ransomware attacks - NCSC.GOV.UK	
• Provide awareness training for staff to recognise, report, and appropriately respond to security messages and/or suspicious activities.	

Acceptable Use

Checklist	Completed
Ensure all users have read the relevant policies and signed IT acceptable use and loan agreements for school devices.	

Communicating the Plan

Checklist	Completed
Communicate the Cyber Recovery Plan to all those who are likely to be affected and be sure to inform key staff of their roles and responsibilities in the event of an incident, prior to any issue arising.	Y

Artificial Intelligence (AI)

Veritas MAT is committed to reviewing the opportunities generative AI can bring to support the education sector and our staff workloads and pupil learning across the Trust. The capabilities AI can bring also present challenges for the safeguarding and security of our filtering and monitoring processes. Veritas MAT will review any potential AI products to ensure the appropriate levels of filtering and monitoring are in place within the product and on top of any AI product, ensuring all users are effectively protected from generating or accessing harmful or inappropriate content and meet the guidelines outlined in Keeping Children Safe in Education, Filtering and Monitoring Standards for Schools and Colleges and the Online Safety Act 2023 as well as General Data Protection Regulation (GDPR) and ICO age appropriate design code.

Veritas MAT will continue to review this policy in line with developments of AI within the education sector and any possible implementation of this across the Trust.