DATA PROTECTION & INFORMATION SYSTEMS

Achieve + Learn Trust.
Better, together.

Cyber Security Policy

Approved by:	Board of Trustees
Date:	November 2024
Date of Next Review:	November 2025

OUR VALUES

AMBITION	We instil a lifelong love of learning and nurture skills and talents
INCLUSION	We welcome and respect people from all backgrounds, valuing and celebrating diversity
ASPIRATION	We want people to be the best they can be, and for everyone to achieve their potential
COMMUNITY	We develop local and global citizens for the future, always committed to working in partnership
BELIEF	We encourage everyone to believe in themselves and their future, providing opportunities to excel

Our Vision

Our vision is to make sure all students get the best educational experience. This means that alongside our broad and aspirational curriculum, we offer students diverse enrichment opportunities to help them find their passions.

It's important to us that students grow both academically and personally. To do this, we create safe, inclusive and enriched learning environments in our schools, with opportunities outside of the classroom that open up pathways to successful futures.

We respect each school's individuality and the communities you serve, so we'll work with you to support your development without changing your identity. Our network of schools collaborate and share knowledge to provide exceptional learning experiences and more opportunities for students to find what they love, and what they're good at.

Our Aims

Our aim is to ensure that all schools within the trust aspire to be 'outstanding' and hold a minimum of a 'good' rating in all categories from Ofsted.

Our Future

We strive for continuous improvement and development. Our expansion will create and nurture a strong partnership of schools, covering both primary and secondary phases. Simply put, we believe that we are better, together. Working collaboratively allows us to build on each school's strengths, while supporting areas of improvement.

Our Governance

The Members of the Trust are the signatories to the Trust's Memorandum and Articles of Association and are responsible for approving any amendments to the Articles. Members have a distinct but limited role, but it is, however, an incredibly important one. In summary, the role of Members is to act as the 'guardian' for the effective operation of the Trust assuring themselves that the Board is exercising effective leadership and governance of the organisation.

In addition to the trust board, each member school has its own local governing body.

Contents

		Page
1	Purpose and Scope	4
2	Responsibilities	5
	2.1 School I.T. Department Responsibilities	
	2.2 Staff Responsibilities	
3	Firewalls	6
4	Endpoint Protection	6
5	Updates and Patches	6
6	Email Communications	7
7	Passwords	8
8	Sharing of Data	8
9	Additional Measures	9
10	Personal Devices	9
11	Remote Working	10
12	Cyber Incidents	10

1 Purpose and Scope

Achieve and Learn Trust takes its responsibilities with regards to cyber security and ensuring the safety and integrity of its Information Technology systems seriously:

Achieve and Learn Trust also recognises that I.T systems are an integral part of the smooth and efficient running of a school and that it is important to ensure that these systems are protected against external and internal threats.

This policy sets out the accountability and responsibilities of the school, it's staff, students and governors to fully comply with cyber security regulations and guidelines set out by the Department for Education (DfE) and National Cyber Security Centre (NCSC).

Schools within the Achieve and Learn Trust utilise and manage a variety of I.T. systems which are hosted either on-premises or in the cloud. These systems are used by Staff, Students and Governors, defined as "Users".

This policy therefore seeks to ensure that we:

- Continue to ensure the security and integrity of all school managed systems
- Have a clear and thorough understanding of our responsibilities
- Comply with cyber security regulations and best practices

This policy applies to all systems which are managed and maintained by the school's I.T department whether that be on premise or hosted in the cloud.

All users of any school I.T. system must comply with this policy. A failure to comply with this policy may result in disciplinary action being taken.

2 Responsibilities

2.1. School I.T Department Responsibilities

The School's I.T. department is responsible for:

- Installing and maintaining firewalls, anti-malware software and authentication systems in accordance with regulations and best practices set out by the vendors of each respective system.
- Ensuring that the school's cyber security provisions are active and functioning correctly.
- Regularly reviewing the school's cyber security provision to ensure that it remains effective.
- Ensuring that the school's cyber security response plan is kept up to date
- Arranging annual cyber-security for all school staff
- Keeping users informed and up to date with information on the latest threats, scams and phishing emails and provide advice on how to combat them.
- Investigate all suspected security threats thoroughly and liaise with the relevant authority where necessary.
- Following the provisions laid out in this policy in the same way other users do.
- Ensuring that backups of data are functional and are kept safe and secure and are not openly vulnerable to threats.
- Ensuring that their day-to-day user credentials are not granted elevated permissions and that separate admin accounts are used to administer systems.
- Performing regular tests of security and protection systems to assess response and effectiveness in the event of a cyber security incident.

2.2. User Responsibilities

Staff, Students and Governors who use school I.T. systems are responsible for:

- Ensuring that they use school I.T. systems in accordance with this policy.
- Reporting any confirmed or suspected cyber incidents
- Ensuring that they keep their school or Trust access credentials safe and secure
- Ensuring they their own personal devices do not pose a cyber risk to school or Trust I.T systems if they are used to access resources.
- Keeping any school or Trust issued devices safe

3 Firewalls

Achieve and Learn Trust schools operate a physical hardware firewall between their network and the internet as well as a software-based firewall which is configured on all school managed workstations and servers. The purpose of the firewall is to manage the data being transferred to and from a device or network and only allow legitimate and required traffic.

On school owned devices, the firewall is managed by the school's I.T. department. If a user suspects that a firewall is not functioning correctly, they should contact the school's Network Manager.

4 Endpoint Protection

Achieve and Learn Trust schools install anti-virus protection software on all workstations and servers managed by the school. The purpose of this is to protect the system from malicious software such as viruses, malware or ransomware.
The school I.T. department will ensure that the virus signatures used by the software are constantly up to date. If a user suspects that the anti-virus software is not up to date or functioning correctly, they should contact the school's Network Manager.

5 Updates and Patches

Achieve and Learn Trust recognises that vulnerabilities in computer systems and software are discovered regularly. Software companies regularly release software updates and patches to counteract these vulnerabilities. These patches must be installed to ensure that devices remain protected from threats. Out of date, unpatched and unsupported software increases the vulnerability of a computer system to cyber threats.

The school's I.T. department will ensure that all software on school devices is updated in a timely manner and in accordance with the vendor's recommendation.

6 Email Communication

Achieve and Learn Trust recognises that email communications are often the chosen transport method of scammers and distributors of malicious software (e.g. worms, trojans and viruses).
To avoid infection from malware and to avoid data theft and / or loss, users should:

- Avoid opening and clicking on links from senders who they do not recognise or when the content of the link is not explained clearly.
- Avoid opening links in emails which they are not expecting.
- Check the names and email addresses of senders to ensure emails are legitimate.
- Check for inconsistencies or “give-aways” in email content (e.g. grammar mistakes, spelling mistakes etc.)
- Pay attention to “Mail-Tips” and the external sender warning.
- Report any suspicious communication via the “Report Phishing” button in Outlook or via the IT Helpdesk.
- Report the clicking on or accessing of a potentially malicious link to the school’s I.T. department immediately.
- If in doubt, check whether a message is legitimate or not with a member of the I.T. Department.

Achieve and Learn Trust also recognises that cyber incidents relating to emails can also originate within the organisation, this includes an email being sent to the wrong recipient or the sharing of data without the correct security precautions being taken.

When sending emails, users should:

- Ensure that all recipients of the email are correct
- If an email has multiple recipients addressed or CC’d, users must ensure that all recipients are authorised to receive the information contained in the email.
- Pay attention to any “Mail-Tips” which appear

In the event a cyber incident occurs because of the sending or receiving of an email, the user must inform the school Network Manager.

7 Passwords

Achieve and Learn Trust recognises that credential leaks are highly dangerous and that they can compromise the integrity and security of a school's I.T. systems and lead to further data loss and risk other systems becoming compromised.
Passwords used to access school systems should be devised in such a way that they cannot be easily guessed or hacked. For this reason, users are instructed to:

- Use a password which contains at least 8 characters including capital letters, numbers and special characters.
- Avoid using passwords which can be easily guessed (e.g. birthdays)
- Never share credentials with any other party and only access school I.T. systems using their issued credentials.
- Avoid writing passwords down in notebooks or on post-it notes, if a password must be documented, use a trusted and reputable password manager.
- Use multi-factor authentication where available. The use of multi-factor authentication will be enforced where possible.

8 Sharing of Data

Achieve and Learn Trust recognises that at times it may be necessary for data to be shared externally.

When the need to share data arises, users must ensure that:

- They have authority to share the data.
- The content being shared is proportionate to the purpose of sharing the data.
- It is necessary for the data to be shared.
- They have taken all reasonable steps to ensure the safety and security of the data being shared.
- Access to the data is available only to the required recipients.

Achieve and Learn Trust requires that all data shared externally, including between Trust schools, be shared using approved platforms only (e.g. Microsoft365) and that the security settings are proportionate to the confidentially of the data. Users are encouraged to seek advice from the school's I.T. department to ensure that data is shared correctly and in accordance with this policy.

9 Additional Preventative Measures

Achieve and Learn Trust requires that users:

- Avoid leaving workstations unlocked when unattended
- Report a perceived threat or possible security weakness in a school I.T. system to the school's Network Manager in a timely manner.
- Report lost or stolen equipment immediately to the school's Network Manager.
- Refrain from accessing suspicious websites.
- Refrain from downloading suspicious, unauthorised or illegal content on school devices.
- Contact the school's I.T. department immediately if they suspect an account has been compromised and change all passwords immediately.

10 Personal Devices

Achieve and Learn Trust acknowledges that users may wish to access school resources via their own personal devices when working remotely. When this is the case, users should take steps to ensure that their device does not pose a threat to their own data as well as school or Trust data as security precautions which would normally be managed by the school I.T. department are the responsibility of the device owner.

Users must ensure that:

- Their device has up to date anti-virus software installed and operational.
- Their device is running a supported operating system which is receiving regular security updates.
- They have a firewall enabled and working correctly.
- They do not store confidential school or Trust information on the local storage of their personal device or their personal cloud services.
- If using a shared device with other people such as friends or family members, steps are taken to prevent unauthorised access to school or Trust data.
- They only access and work on school or Trust data on an approved platform such as Remote Desktop Services or Microsoft365.

If a user wishes to bring a personal device to an Achieve and Learn Trust school and access the internet, they must use a dedicated BYOD (Bring Your Own Device) or Guest network. Personal devices must not be connected to the school network ether wirelessly or with a wired connection. Users should contact the school I.T. department if they require assistance in accessing the correct network.

11 Remote Working

Achieve and Learn Trust recognises that at times there is a need for both staff and students to work remotely, this includes via Remote Desktop Services (RDS) or on cloud-based platforms such as Microsoft 365. When users are accessing any system managed by an Achieve and Learn Trust school, they are obliged to follow the same practices and procedures they would if using a school device.

When working on a network that is not managed by the school's I.T Department, users should be aware that the network could be less secure, this includes networks at home, in another school or in a public place such as a coffee shop or hotel.

Devices issued by the school will continue to be protected by a firewall and anti-virus software whilst working remotely.

Users must only work remotely using approved methods such as via Remote Desktop Services (RDS) or Microsoft365 and any data must remain on the platform or device provided by the school and not downloaded to a personal device for editing.

When in a public place, users must remain aware of their surroundings when working on confidential data or when entering credentials to access school I.T. systems and ensure that this information cannot be seen by unauthorised persons.

12 Cyber Security Incidents

Achieve and Learn Trust recognises a Cyber Incident as any breach of a computer system, this includes infection by malware, a person having access to data which they should not be able to access or a complex cyber incident which may cause a system to be unavailable.

Achieve and Learn Trust expects all users to report cyber incidents. If a user becomes aware of a confirmed or suspected cyber incident, they should report this immediately to the school's Network Manager.