For the purposes of this policy, 'the Trust' refers to The Trust and all schools within the Trust.

Cyber Security Policy

Monitoring and review	
Author	Tanya Marley
Approver	Trustees
Owner	Tanya Marley, Director of Estates and Operations
Most recent review date:	May 2026
Date of next review	**May 2027**
Review frequency:	One Year
Category of policy	Statutory
Who has been consulted	James Garnett, Independent IT Consultant
ADAPT or ADOPT	ADAPT

Version History Log

Version	Description of Change	Amended by	Date
1	Initial issue		1 September 2025
2	Brookfields Adaptations	CBE	October 2025
3	Reviewed – minor change. Added under section 7: 'Where available, password-based authentication will be supported by multi-factor authentication, in line with current NCSC guidance.'	TMA	May 2026
3.1	Updated by Brookfields to V3	SMR	June 2026

Ascendancy Partnership Trust

CONTENTS

1. Introduction

Cyber security has been identified as a risk for the Trust and every employee needs to contribute to ensure data security.

The Trust has invested in technical cyber security measures, but we also need our employees, Trustees, Governors and volunteers to be vigilant and to act to protect the Trust IT systems.

[See Appendix A for details of person responsible for cyber security within individual schools]
If you are an employee, you may be liable to disciplinary action if you breach this policy.

This policy supplements other data management and security policies.

2. Purpose and Scope

The purpose of this document is to establish systems and controls to protect the Trust from cyber criminals and associated cyber security risks, as well as to set out an action plan should the Trust fall victim to cyber-crime.

This policy is relevant to all staff, trustees, governors and volunteers.

3. What is Cyber-Crime?

Cyber-crime is simply a criminal activity carried out using computers or the internet including hacking, phishing, malware, viruses or ransom attacks.

The following are all potential consequences of cyber-crime which could affect an individual and/or individuals:

- Cost - The global cost of all forms of online crime is estimated to be in excess of £300 billion. We may be fined up to £17.5 million or 4% of the total worldwide annual turnover if we fail to protect our data.
- Confidentiality and data protection - Protecting individuals' confidential information and all forms of personal data is one of the most essential requirements for our school. The risk of compromise or loss of access to confidential information and personal data is the biggest of all threats from cyber-crime.
- Potential for regulatory breach - We have various regulatory duties which we could unintentionally breach through falling victim to cyber-crime or a cyber-attack. Loss of personal data can lead to claims for damages by the individuals concerned and/or significant fines from the Information Commissioners Office (ICO).

- Reputational damage – A cyber security incident can have a major impact on our reputation, particularly if it involves the loss of confidential information, personal data and/or is reported in the media. Protecting our reputation is of utmost importance.

- Business interruption – Some forms of cyber-attack could render key systems (for instance servers including email servers, cloud computing services or our website) unavailable. This would have a major impact on delivering lessons and delivering our services. It may be necessary in such cases to invoke our Business Continuity Plan. In reality as other organisations have experienced the loss of IT systems can last weeks. [Appendix A] is responsible for making that decision and communicating with IT.

- Structural and financial instability – The financial losses flowing from online crime may cause or contribute to financial difficulty, this could include fewer pupils due to reputational damage and financial loss due to fraud or fines all of which will have a significant impact on the Trusts financial position.

4. Cyber-Crime Prevention

Given the seriousness of the consequences noted above, it is important for the Trust to take preventative measures and for staff to follow the guidance within this policy.

This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime. [See Appendix A] for the contact person who can provide further details of other aspects of the Trust/School risk assessment process upon request.

The Trust has put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance for staff.

5. Technology Solutions

The Trust have implemented the following technical measures to protect against cyber-crime:

- firewalls
- anti-virus software
- anti-spam software
- auto or real-time updates on our systems and applications
- URL filtering
- secure data backup
- encryption
- deleting or disabling unused/unnecessary user accounts
- disabling accounts immediately a user leaves the Trust

- deleting or disabling unused/unnecessary software
- using strong passwords; and
- disabling auto-run features.

The Trust will be addressing the lack of Multi Factor Authentication (MFA) and geo-fencing, which restricts the countries staff can log in from,

The Trust are reviewing how unsecure accounts, i.e. shared accounts can be accessed out of school.

6. Controls and Guidance for Staff

- All staff must follow the policies related to cyber-crime and cyber security as listed in this policy.
- Technology solutions in isolation cannot protect us adequately, so our systems and controls extend to cover the human element of cyber-crime/cyber security risk.
- All staff will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the Trust or any third parties with whom we share data.
    - We will implement a policy of least privilege such that staff are only given access to the information they need to undertake their role by applying security permissions based on job role in the Trust or school. We expect staff to: sign the confidentiality agreement and Acceptable Use Policy; observe the Trust's clear desk policy; dispose of confidential documents securely; not read confidential papers which can be read by members of the public or discuss sensitive matters where you can be overheard.
    - We will also implement, where appropriate, physically ringfencing individuals or team working in sensitive data; processes for ensuring sensitive incoming correspondence is not shared inadvertently; and other measures to protect staff and pupil data
- Due diligence – we may conduct due diligence on the cyber security controls and cyber-crime prevention measures that other parties with whom we share information.

All staff must:

- Ensure you are familiar with the risks presented by cyber-crime and cyber security attacks or failures and take appropriate action to mitigate the risks by taking a sensible approach, e.g. not forwarding chain letters or inappropriate/spam emails to others. We

will help you by continually raising awareness of those risks and providing training where necessary.

- Report any concerns you may have.

7. Passwords

Choose strong passwords e.g. Combinations of unconnected words are best (ideally 3 but 2 are OK) such as Apple.Blue.26 or Table42Sunny, Apple.Blue.Table or Table4Cloud4Leaf. Where available, password-based authentication will be supported by multi-factor authentication, in line with current NCSC guidance.

- Keep passwords secret
- never reuse a password
- All staff are required to read and adhere to the Acceptable Use Policy annually.
- not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on their computer, phone or network or the Trust IT systems
- report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to [See Appendix A] as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our Data Breach Policy
- only access work systems using computers or phones that the Trust owns. Staff may only connect personal devices to the public and/or visitor Wi-Fi provided
- not install software onto your work computer or phone. All software requests should be made to The IT Manager
- avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using Trust equipment and/or networks.

The Trust considers the following actions to be a misuse of its IT systems or resources:

- any malicious or illegal action carried out against the Trust or using the Trust's systems
- accessing inappropriate, adult or illegal content within the Trust premises or using the Trust equipment
- excessive personal use of the Trust's IT systems during working hours
- removing data or equipment from the Trust premises or systems without permission, or in circumstances prohibited by this policy

- using the Trust equipment in a way prohibited by this policy
- circumventing technical cyber security measures implemented by the Trust's IT team; and
- failing to report a mistake or cyber security breach
- Downloading or copying Trust programs or software to personal IT systems

8. Cyber-Crime Incident Management Plan

The incident management plan consists of four main stages:

1. *Containment and recovery:* To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost. We will notify our insurers as soon as reasonably practicable of any circumstances that may give rise to claim under relevant insurance policies. We will also assess whether it is necessary to invoke our business continuity plan.
2. *Assessment of the ongoing risk:* To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed, and any consequences of the breach/attack identified.
3. *Notification:* To consider whether the cyber-attack needs to be reported to regulators (for example, the ICO and National Crime Agency) and/or colleagues/parents as appropriate.
4. *Evaluation and response:* To evaluate future threats to data security and to consider any improvements that can be made.

Where it is apparent that a cyber security incident involves a personal data breach, the Trust will invoke their Data Breach Policy rather than follow out the process above.

Appendix A: Contacts

Responsibility	Contact	Job Title
Cyber Security	Matt Slingsby mslingsby@brookfields.w-berrks.sch.uk	IT Manager
Business interruption – decision to involve business continuity plan	Catherine Bernie cbernie@brookfields.w-berks.sch.uk	Headteacher
Provide details of risk assessments	Catherine Bernie cbernie@brookfields.w-berks.sch.uk	Headteacher
Receive reports of Cyber Security breaches	Matt Slingsby mslingsby@brookfields.w-berrks.sch.uk Catherine Bernie cbernie@brookfields.w-berks.sch.uk	IT Manager Headteacher