ACACIA NURSERY SCHOOL
growing excellence

Cyber Security Policy

September 2025

Signed (Chair of Governing Body):	[redacted]
Date:	**September 2025**
Date of Review:	September 2026

As part of a formal Service Level agreement between the Local Authority, Arbor Academy Trust and the Acacia Nursery School Governing Body, the Governing Body has adopted this policy. The Governing Body reviews this policy annually.

The governors may, however, review the policy earlier than this, if the Government introduces new regulations, or if the Governing Body receives recommendations on how the policy might be improved. This document is also available in other formats e.g. e-mail and enlarged print version, on request to the School Office and is displayed on the school's website.

Introduction

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

The school has invested in technical cyber security measures but we also need our employees to be vigilant and to act to protect the School IT systems.

The school shall be registered with an authorised National Cyber Security Centre auditor to maintain the Cyber Essentials certification annually.

The Nursery lead is responsible for cyber security within the school.

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, namely our Data Protection Policy, Data Breach Policy, Information Security Policy, Acceptable Use Policy, Home Working Policy, Electronic Information and Communications Policy and Clear Desk Policy.

Purpose and Scope

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

This policy is relevant to all staff and Governors.

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;
- confidentiality and data protection;
- potential for regulatory breach;
- reputational damage;
- business interruption; and

- structural and financial instability.

Cyber-Crime Prevention

Given the seriousness of the consequences noted above, it is important for the school 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. The Head of School can provide further details of other aspects of the school risk assessment process upon request.

The school have 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.

Technology Solutions

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

(i) firewalls;

(ii) anti-virus and malware software;

(iii) anti-spam software;

(iv) auto or real-time updates on our systems and applications;

(v) URL filtering;

(vi) secure data backup;

(vii) encryption;

(viii) deleting or disabling unused/unnecessary user accounts;

(ix) deleting or disabling unused/unnecessary software;

(x) using strong passwords; and

(xi) using 2 form factor verification for staff; and

(xii) disabling auto-run features.

Controls and Guidance for Staff

- All staff must follow the policies related to cyber-crime and cyber security as listed in this policy.

- 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 School or any third parties with whom we share data.

- All staff must:

- Choose a minimum 8 character complex passwords consisting of letters, numbers and symbols;
- keep passwords secret;
- never reuse a password;
- change password regularly or when prompted by the system
- Use 2 Form Factor Verification when enforced
- never allow any other person to access the school's systems using your login details;
- never share your 2 Form Factor backup codes;
- Passwords can only be saved in the school approved system password manager (Google Password Manager);
- 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 School IT systems;
- report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to the Head of School 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 School owns. Staff may only connect personal devices to the visitor Wi-Fi provided;
- Only transmit school data by secure and encrypted means
- not install software onto any School system including computers, phones or cloud systems. All software requests should be via a business case made to the Head of School; and
- avoid clicking on links within emails, messages, or general browsing to unknown websites, downloading large files, or accessing inappropriate content using school equipment and/or networks.

  - avoid leaving sensitive or personal data on printers, computer monitors or desk whilst away from your desk or computer

- The school considers the following actions to be a misuse of its IT systems or resources:
  - any malicious or illegal action carried out against the school or using the school's systems;
  - accessing inappropriate, adult or illegal content within School premises or using School equipment;
  - excessive personal use of School's IT systems during working hours;
  - removing data or equipment from School premises or systems without permission, or in circumstances prohibited by this policy;
  - using School equipment in a way prohibited by this policy;
  - circumventing technical cyber security measures implemented by the School's IT team; and
  - failing to report a mistake or cyber security breach.

Disposal of IT Systems Equipment

- The school shall ensure any personal data or software is obliterated from devices if the recipient organisation is not authorised to receive the data contained on the equipment being disposed.
- It is important to ensure that any software remaining on a device being relinquished for reuse is legitimate. Care should be taken to avoid infringing software and data copyright and licensing restrictions by supplying unlicensed copies of software inadvertently.
- The school shall ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.

Asset Management Systems

To ensure that security controls to protect the data and systems are applied effectively, Acacia Nursery School will maintain asset registers for, files/systems that hold confidential data, and all physical devices (servers, switches, desktops, laptops etc) that make up its IT services.

System Security Design and Planning

Levett Consultancy will build security principles into the design of IT services for Acacia Nursery School covering but not limited to:

- Security patching – network hardware, operating systems and software
- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them
- Actively manage anti-virus systems

- Actively manage and test backups
- Regularly review and update security controls that are available with existing systems
- Segregate wireless networks used for visitors' & staff personal devices from school systems
- Review the security risk of new systems or projects

Cyber-Crime Incident Management Plan

The incident management plan consists of four main stages:

(i) *Containment and recovery:* To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost.

(ii) *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.

(iii) *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.

(iv) *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 School will invoke their Data Breach Policy rather than follow out the process above.