CYBER SECURITY POLICY

Policy Reference	Cyber Security
Committee	
Completed Review Date	8th May 2025
Policy Owner	Data Protection Lead – Jane Selvey
Ratified by Governors	
Next Review Due	May 2026

Signed by Principal	
Signed by Chair of Governor	

MONITORING, EVALUATION AND REVIEW

This policy will be reviewed when there are changes in the law or at least every two years, to assess implementation and effectiveness in line with DfE guidance September 2022.

This policy will be promoted and implemented throughout the Academy.

Contents

Version History Log

Version	Description of Change	Date of Policy Release by Judicium
1	Initial Issue	19.10.21
2	Formatting amendments	03.08.22
3	Included details of cyber crime, technology solutions, controls and guidance for staff.	30.08.24

1. 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.

Advanced IT Services Nottingham LTD is the school's IT Provider and are responsible for cyber security within the School. This is overseen by the school Data Protection Lead, and interim reviews are scheduled to ensure that we are following best practice guidelines and any industry governance and/or compliance measures.

If you are an employee, you may be liable to disciplinary action if you breach this policy. All employees must review this policy and acceptance on a yearly basis, and/or when updates are made.

This policy supplements other data management and security policies, namely our Data Protection Policy, Data Breach Policy, Information Security Policy, Acceptable Use Policy.

2. 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, Governors, students and volunteers within the school environment who have access to school systems; for example a network login or school email address.

3. Governance and Roles

Effective cyber security depends on clearly defined responsibilities and governance. The following roles are accountable for the management, oversight and implementation of cyber security measures.

Strategic Leadership

The Headteacher is accountable for the overall implementation of this policy and ensuring cyber risks are considered a part of strategic and operational planning. The headteacher is responsible for:

- Approving this policy and ensuring it is implemented
- Promoting a culture of cyber awareness and responsibility
- Ensuring cyber risks are considered within broader risk management and safeguarding frameworks
- Supporting the allocation of appropriate resources to manage cyber security risks

Data Protection Officer (DPO)

The school's DPO oversees personal data handling. The DPO is responsible for:

- Ensuring compliance with UK GDPR and the Data Protection Act 2018
- Overseeing personal data handling and breach response
- Liasing with regulatory bodies (e.g. ICO) when required
- Providing guidance on data security risks associated with cyber threats
- Working with IT support to coordinate responses to incidents involving personal data

The schools name DPO is: Judicium Education

IT Support Partner (Advanced IT Services, Nottingham)

AIT is the school's managed IT service provider, responsible for the technical delivery of cyber security controls:

Their responsibilities include:

- Implementing and maintaining technical safeguards (e.g., firewalls, antivirus, patch management etc)
- Monitoring systems for suspicious activity and responding to incidents
- Managing user access and device security
- Providing technical advice and support for school-led security initiatives
- Maintaining compliance with Cyber Essentials, DfE Standards and IISO27001-aligned controls

The IT provider reports regularly to the school's senior leadership team on system performance, risks and incidents. Any cyber related concerns or queries should be reported immediately to Advanced IT Services via help@advanceditservices.co.uk

Designated Safeguarding Lead (DSL)

The DSL ensures that cyber security is aligned with safeguarding duties. Their responsibilities are:

- Identifying cyber threats that may impact student safety (e.g., online harm, grooming, exploitation)
- Working with IT and teaching staff to reinforce digital safety in the curriculum
- Supporting students affected by cyber incidents

The school's appointed DLS(s) are/is:

All staff and System Users

Every individual using school systems or data plays a vital role in maintaining security. All users must:

- Follow the Cyber Security Policy and Acceptable Use Agreements
- Protect passwords and secure devices. Users should not share accounts or disclose passwords to anyone

- Be alert to phishing, scams and suspicious behaviour
- Complete mandatory training
- Report actual or suspected breaches immediately

Cyber security is everyone's responsibility. All users who interact with the network have a responsibility to ensure they remain vigilant when using school devices, associated systems or infrastructure.

Should an account be compromised, or a user have a cyber incident to report or query, please contact Advanced IT Services immediately: help@advanceditservices.co.uk or 0115 9170 197

4. 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 our school. The risk 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. The Principal 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.

5. 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. Advanced IT Services Nottingham LTD can provide further details of other aspects of the School/Trust 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.

6. Technology Solutions

The school has adopted a **defense-in-depth** approach to cyber security, implementing a layered system of technical safeguards to prevent, detect, and mitigate cyber threats. These controls are designed to meet the requirements of **Cyber Essentials**, support alignment with **ISO/IEC 27001**, and comply with the **DfE Digital and Technology Standards**.
All controls are managed and regularly reviewed termly, or as new standards or risks evolve by the school's IT support partner Advanced IT Services, in coordination with the senior leadership team and the DPO.

- **Perimeter firewalls** are in place to control incoming and outgoing network traffic.
- **Internal network segmentation** separates administrative, curriculum, and guest traffic.
- **Port filtering and IP whitelisting** is used to restrict access to critical infrastructure.
- **Wireless networks** are protected using WPA2/WPA3 encryption and require authentication.
- **Public and guest Wi-Fi** is logically isolated from staff and student networks.

User Access Control

- All users are issued with unique accounts tied to role-based permissions.
- **Principle of least privilege** is applied; users only have access to the data and systems they need.
- **Multi-Factor Authentication (MFA)** is enabled on all applicable services, especially email, remote access, and administrative consoles.
- **Account lifecycle management** ensures prompt deactivation of leavers and periodic auditing of user access.
- **Administrator privileges** are restricted to IT support staff and monitored for misuse.

Device and Endpoint Security

- All school-owned devices are managed centrally through endpoint management tools
- **Antivirus and anti-malware protection** is installed and kept up to date across all endpoints.
- **Encryption** is enabled for all mobile and portable devices, including staff laptops and USB drives.
- **Remote wipe capability** is enabled on mobile devices used for school business.
- **Auto-lock, inactivity timeouts, and secure boot** are configured to prevent unauthorised access.
- Devices are patched within 14 days of a security update being released, in line with **NCSC 14 Cyber Security Principles**.

Application and Cloud Security

- Applications are approved and vetted before installation to ensure compliance and security.
- **Software updates and patches** are applied promptly to mitigate known vulnerabilities.
- The school uses **cloud-based platforms** (e.g. Microsoft 365, Google Workspace) with appropriate security configurations, including MFA, data loss prevention (DLP), and conditional access.
- **Legacy and unused software** is uninstalled or disabled to reduce attack surface.

Email and Web Filtering

- **Advanced email filtering** is deployed to detect and block phishing, spoofed domains, and malicious attachments.
- **URL and web content filtering** prevent access to inappropriate or high-risk websites.
- All inbound and outbound email is scanned for malicious content and policy violations.
- Email systems include **spoofing and impersonation protection** through SPF, DKIM, and DMARC records.

Backup and Disaster Recovery

- Secure, encrypted **offsite and cloud-based backups** are taken regularly and include critical systems, documents, and MIS data.
- Backups are tested periodically for integrity and recovery readiness.
- Backup systems are configured with **immutable storage** where supported to guard against ransomware tampering.
- The school has a tested **Disaster Recovery and Business Continuity Plan** aligned with DfE guidance.

Logging and Monitoring

- **System event logs** are collected from key infrastructure and cloud services.
- Logs are monitored for suspicious activity, anomalies, or policy violations.
- Alerts are configured for priority events such as failed login attempts, privilege escalation, or malware detection.
- The school retains logs in line with its Data Retention Schedule and relevant data protection laws.

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

- It may be appropriate in some instances to limit the number of people involved or who have access to information on a matter to ensure the security of the data involved. This can be part achieved through IT security measures. We may implement other controls that are more practical in nature, e.g.:

- Physically ringfencing the individuals or teams working on a matter;

- Taking steps to ensure our system for opening, distributing and/or scanning incoming correspondence (by post, email or otherwise) does not allow or inadvertent sharing of confidential information;
- Getting a signed confidentiality agreement from each staff member;
- Disposing of confidential documents securely;
- Having a clear desk policy;
- Discouraging staff from reading confidential papers or discussing sensitive matters in public.

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.
- **Passwords**
    - Choose strong passwords (the School's IT team advises that a strong password contains a combination of upper and lowercase letters, special characters and be a minimum of 12 characters in length. All passwords must;
    - keep passwords secret;
    - never reuse a password;
    - never allow any other person to access the school's systems using your login details;

- 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 schools Data Protection Lead 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.;

- not install software onto your School computer or phone. All software requests should be made to Advanced IT Services Nottingham (AIT) via the helpdesk ticketing system in writing to help@chacademy.co.uk

- avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using School equipment and/or networks.

- 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.

8. Cyber-Crime Incident Management Plan

Despite robust technical controls and training, no system is immune to cyber threats. An effective, timely, and coordinated response to cyber incidents is essential to limit harm, protect data, and restore services quickly. This section outlines how the school responds to suspected or confirmed cyber security incidents.

What is a Cyber Security Incident?

- A cyber incident includes, but is not limited to:
- A phishing or malware attack
- Ransomware infection or encryption of school files
- Compromised user account or unauthorised access to systems
- Data breach involving personal or confidential information
- Service disruption (e.g. Denial of Service or email outage)
- Discovery of suspicious software, behaviour, or unauthorised devices
- Loss or theft of a device containing sensitive school data

Immediate Actions (Detection and Containment)

All users are responsible for reporting actual or suspected incidents immediately to:

- The IT Support Provider (Advanced IT Services). Incidents can be reported to 0115 9170 197, and via email to help@advanceditservices.co.uk. For emergency incidents, this can be reported to the P1 email (24/7/365 monitored) support@advanceditservices.co.uk
- The School's Data Protection Officer (if personal data is involved). The schools DPO can be reached via [INSERT EMAIL]

Users should **not attempt to investigate or contain the incident themselves**, as this may risk damaging evidence or worsening the impact.

IT support will take the following steps:

- Isolate affected devices or accounts (e.g. disable logins, disconnect from the network)
- Preserve logs and system data for investigation
- Conduct preliminary triage to understand the scope and scale
- Notify the Headteacher and DPO of significant incidents

Where appropriate, the school may also notify relevant stakeholders such as:

- The DfE Incident Support Line
- National Cyber Security Centre (NCSC)
- Action Fraud / National Crime Agency (NCA)
- Insurers, if a claim may be triggered

Assessment and Impact Evaluation

The incident response team (IT, SLT, DPO) will:

- Confirm what happened, when, and how
- Identify which systems, users, and data were affected
- Determine whether personal data was compromised and, if so, how sensitive it was
- Assess the ongoing risk to school operations and individuals

- Evaluate whether the Business Continuity Plan needs to be invoked

Where personal data is involved, the incident will be escalated under the school's Data Breach Policy, and the DPO will determine if notification to the Information Commissioner's Office (ICO) is required within 72 hours.

Communication and Notification

Depending on the nature of the incident, the school may need to:

- Inform affected individuals (e.g. staff, students, parents)
- Notify third-party service providers or partners
- Liaise with law enforcement, local authority, or regulators
- Issue internal or external communications (e.g. parent bulletins, press responses)

All communication will be coordinated through senior leadership in consultation with legal or data protection advisors where needed.

Recovery and Restoration

Once the threat has been contained:

- Systems will be restored from secure, verified backups
- Compromised accounts will be reset and resecured
- Any vulnerable software or misconfigurations will be patched or removed
- Root cause analysis will be conducted to prevent recurrence
- Staff and students will be supported through any required actions (e.g. password resets, device reimaging)
- The school will avoid paying ransoms under any circumstance, in line with NCSC and law enforcement advice.

Lessons Learned and Continuous Improvement

After each incident, a post-incident review will be conducted to evaluate:

- Response effectiveness
- Gaps in technology, training, or process
- Additional controls required
- Lessons to feed into future awareness campaigns or updates to this policy

This review will be documented and shared with relevant stakeholders, and outcomes will inform updates to the school's risk register, training programme, and business continuity planning.

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.

9. Monitoring and Compliance

Cyber security monitoring is carried out in partnership with Advanced IT Services and includes:

- Real-time alerting for priority events
- Regular audit of access permissions and endpoint security

- Threat intelligence updates from DfE, NCSC, and trusted sources
- Tracking training completion and policy compliance

Non-compliance with this policy may result in:

- Withdrawal of system access
- Disciplinary action
- Referral to external authorities (e.g. ICO) in serious cases

Policy Review

This Cyber Security Policy will be reviewed:

- At least every three years, or sooner where required by:
- Significant changes in legislation or regulatory guidance
- Emergence of new threats or vulnerabilities
- Lessons learned from a major incident or audit finding
- Changes to the school's digital infrastructure or IT service model

The review will be led by the school's DPO and IT provider in consultation with SLT, and formally approved by the Headteacher.