Alban Academies Trust

ICT & Cyber Security Policy

Last Reviewed	March 2023
Reviewed by	Trust Board
Date of Approval	March 2023
Lead responsibility	Director of IT
Next Review	March 2024

Alban Academies Trust	ICT & Cyber Security Policy	
	Last reviewed: March 2023	**Next Review:** March 2024

1 INTRODUCTION

ICT enables and enhances Alban Academies Trust’s educational and organisational vision and objectives. Information stored on school’s ICT assets and related systems represents one of the Trust’s most valuable assets and must be protected to preserve its confidentiality, integrity and availability in order to enable the Trust’s visions and objectives to be achieved.

2 POLICY PURPOSE

The purpose of this Policy is to clarify everyone’s responsibilities and security measures to be undertaken in accordance with regulatory, legislative and local requirements to ensure that information remains confidential, is protected from unauthorised access or disclosure; is accessible and available and that data integrity is not compromised.

3 SCOPE

This Policy is intended for Trust/School owned ICT equipment and systems when held internally or outside a School/Trust’s Central Office. It is intended for anyone who has access to the Trust’s administrative and/or curriculum ICT systems or data.

For this Policy definitions are as follows:

- Information covers any method of information creation or collection, including electronic capture and storage, video and audio recordings and any images.
- ICT or ICT system means computing and communications facilities that support teaching, learning and a range of activities in education.
- ICT is the knowledge, skills and understanding needed to employ information and communication technology appropriately.
- ICT equipment means computers, laptops, Chromebooks, iPads, tablets, cameras and mobile phones.
- Where the term Headteacher is used this incorporates Assistant Headteacher roles where these exist and the CEO of Alban Academies Trust when the statement refers to the central Trust.
- This Policy incorporates the best practice and follows guidance from the National Cyber Security Centre’s ‘10 Steps to Cyber Security’ in the safe and secure storage of electronic files and data (*see* ***Appendix B***).

4 RESPONSIBILITY

The headteachers and governors have ultimate responsibility for setting and enforcing this Policy.

Headteacher’s for schools within the Trust are responsible for ensuring that the requirements relating to this Policy are adopted and adhered to following the information and guidance set out within this Policy through the AAT Director of IT.

The Headteacher alongside the AAT Director of IT has overall responsibility for the implementation of the ICT security arrangements within schools, it is their responsibility to ensure measures are implemented consistently and effectively and is free from discrimination.

The Trust’s Central ICT Team and school’s dedicated on-site IT support team are responsible for ensuring that security measures are installed on ICT systems and regularly monitored for security compliance; advising of any suspected or actual ICT security breaches and ensuring an effective and tested ICT Disaster Recovery Plan is in place.

Everyone who has access to Trust and school's ICT systems and data must comply with this Policy combined with the **AAT IT Acceptable Use & Online Safety (Including Online Safety Acceptable Use Agreements) Policy**.

Any individual outlined and referred to above are required to read, accept and agree to abide with all these policies.

The Trust has produced IT Standards which cover its expected cyber security mechanisms and checks that schools must comply with in order to protect personal data as outlined by the General Data Protection Regulation.

5 ICT ASSET ACCOUNTABILITY AND CONTROL

Procurement

- Procurement of ICT equipment, services and software must be coordinated with AAT Central IT Team as an initial first step. Once consulted and agreed at this stage, authorisation from the AAT Central Team for all ICT related purchases will follow.
- An ICT Asset Register will be maintained by each school's IT Support Team under whose responsibility the ICT equipment is placed. All items will be accounted for annually. In addition, a software and licence register is kept and updated for all schools within the Trust.
- No software which will be used to process personal data should be purchased before a Data Protection Impact Assessment has been undertaken and the Data Map updated.

Repairs and Relocation

- Users are required to contact their school's ICT Support Team to report any faults or problems they experience, whether hardware or software related.
- Connection, disconnection or relocation of any ICT equipment must be undertaken by and/or in consultation with the school's ICT Support Team.
- Damaged or faulty devices must not be used under any circumstances and should be returned or reported immediately to the school's ICT Support Team.

Disposal & Loss of ICT Equipment

- ICT equipment identified for disposal or reuse must be held in secure storage until redeployed or disposed of. Disposal information must be recorded and noted on the ICT Asset Register.
- ICT equipment can either be completely wiped clean of data on a school's premises by the school's ICT Support Team or externally by a Waste Electrical and Electronic Equipment (WEEE) accredited compliant recycling partner, which ***must*** provide certificates as evidence of the secure destruction of data.
- Any loss of devices must be immediately reported to the school's ICT Support Team who will arrange instant disablement and security measures of the device when and where possible.

Staff Departure

- All staff who leave the employment of Alban Academies Trust must return Trust/School owned ICT equipment as part of the leaving process.
- Staff are also required to confirm that they have deleted any school related emails, data or files that they may hold on their personal devices.

6 PHYSICAL AND ENVIRONMENTAL SECURITY

- All servers, networks and communications equipment including associated cabling will be located in secure rooms and where possible/required will be climate controlled and housed in appropriate cabinets.

- Access to ICT rooms will be restricted to authorised persons by keycode locks, swipe card access or manually lockable methods.
- Eating and drinking is strictly prohibited when in ICT Suites or when using Trust/School owned devices.

7 EQUIPMENT SECURITY

Equipment Placement and Protection

- Computer screens, keyboards, printers or other similar devices must be positioned so that information stored or being processed can't be viewed by persons not authorised to such information.
- ICT equipment must be positioned so it isn't damaged by dust and heat.
- With the exception of portable and mobile devices provided specifically for home working, employees are not permitted to remove ICT equipment from school/Trust premises.
- Devices must be held securely on and off school's premises.
- All desktop, portable and mobile devices will have a basic input output system (BIOS) password
- Time appropriate automatic screen locking procedures will be implemented for required users in the instance of inactivity over a period of time. A user's password will be required to unlock the screen in this event.
- Staff must ensure that all desktop, portable and mobile devices are locked prior to leaving them unattended.

Power Supplies

Critical hardware such as servers and communications equipment will be protected from power supply failure through the use of uninterruptible power supplies (UPS) which offer battery-based backup power.

Clock Synchronisation

In order to ensure the accuracy of logging and/or monitoring information, the time clocks on the Trust's servers and required ICT devices should be synchronised to a Network Time Protocol (NTP) source.

8 SECURITY OF DATA

All teaching staff and some support staff are in possession of confidential, sensitive and personal data about children and parents/carers and have an explicit duty under law to guard this data and use it appropriately. AAT takes the security of information very seriously and recognises our duties under the new General Data Protection Regulations of 2018. Please see the **AAT GDPR Policy** and individual schools' Data Security Policies for further guidance.

9 ANTI VIRUS

- Anti-virus software is installed onto Trust/school servers and managed on every Trust/school owned networked device.
- Client devices are configured to automatically check and install updates at regular intervals.
- Any Trust owned portable and mobile ICT devices connected to the Internet must be allowed to install automated virus definition and windows security patch updates.
- Non networked ICT equipment e.g. laptops are installed with a standalone copy of anti-virus software which automatically displays a warning message once the virus definition is out of date. Users are required to contact a school's ICT service to arrange regular updates of antivirus software. Laptops must be connected to the school network at least once every 90 days.
- Any information taken from the Internet will be scanned for viruses before it is received on a school's local area network.
- Network devices or software designed to capture and/or analyse network traffic must not be installed on school networks without appropriate authorisation from the Central AAT IT Team.

- External email messages entering a school network will be automatically checked for malware and suspicious content and quarantined if this is the case.
- Where/when a virus is detected, this must be reported immediately to your on-site IT support team or the Central AAT IT Team immediately. In the event of any suspicious content or security breaches on devices, IT will re-image and wipe devices to ensure best practices are followed and to ensure impacted devices are ‘clean’.
- Users who attempt to install, store or use illegal, unapproved or copied software will be subject to appropriate disciplinary action.
- The Central AAT IT Team will implement and utilise Firewall protection to prevent illegal intrusion via the Internet.

10 INFORMATION BACK-UP

Data essential for the day to day running and management of the Trust and school’s is stored on the network server/s and Google cloud-based system. Back-up copies of data will be taken at regular intervals as determined by the AAT Central IT Team and will be taken before any patch or major implementations are applied.

Back-Ups are completed at regular intervals and following best industry practice of the 3-2-1 strategy, where at a minimum two copies are backed up on site and one off site.

Instructions for reinstalling data or files from back-up are fully documented and tested at regular intervals to ensure that they enable the systems and files to be re-loaded in cases of system failure. Data will not be stored on unencrypted portable and mobile devices as these are not included in the automatic back-up of network servers.

Copies of data stored on back-ups are deleted in accordance with the **Trust’s Data Retention Policy**.

11 AUTHORISATION

Only persons authorised by the Trust’s CEO or school’s Headteacher are allowed to use the school's ICT systems. The school’s ICT service will ensure a user is fully aware of the extent to which they may make use of an ICT system. Users will be required to follow the **AAT IT Acceptable Use & Online Safety (Including Online Safety Acceptable Use Agreements) Policy** and **AAT ICT & Cyber Security Policy**.

12 USER PRIVILEGE MANAGEMENT

- Each system will permit access to a user only on entry of a legitimate unique name (User ID) and password. Users must only use their own unique username (User ID) and password to access a school network and not use other staff members profiles.
- Users’ permissions and groups will be set and managed by the AAT Central IT Team, all requests for additional access and permissions must be granted and applied by AAT Central IT Team in conjunction with approval from users line managers or executive staff.
- Only AAT Central IT Team and specific IT Support Staff have administrative privileges on Trust systems.
- AAT Central IT Team restricts user access e.g. to different parts of systems or to view only, view and update or view, update and delete. It also adds or disables user accounts and sets up/amends user profiles.
- Users will only be supplied with the level of access/least privilege required to perform their work duties.
- Users must not attempt to gain access beyond their given access privileges. If additional access is required, permission and approval must be requested and granted.
- In the event of third parties requiring access, they will be provided with accounts that solely provide access to the systems and/or data they are contracted to handle, in accordance with least privilege and need to know principles.
- Third Party accounts will be removed at the end of the contract or when no longer required.

- After entering their unique name (User ID) and password to enter a school ICT system, users will be reminded of their security responsibilities which they must agree to before being able to enter a school network.
- AAT Central IT Team will undertake a systematic review of user profiles on a regular basis to ensure that current access levels are still appropriate, user groups are updated, and that staff are removed/deleted when no longer working within the Trust or if user's requirements change.
- Personal User IDs must not be shared between people and any group
- Access to 'Confidential' and 'Restricted' information will be limited to authorised persons whose roles require it and following the **AAT ICT & Cyber Security Policy**.
- Users who have resigned or no longer contracted will have all access to IT and systems revoked and terminated. In the event of access being required after this period and in unique circumstances, permission must be given by the Trust CEO/COO or Headteacher.
- All ICT equipment on loan to staff must be returned on their final day of employment.
- Users who have been dismissed or subject to disciplinary action or criminal charges which may compromise the security of information systems must not have access to Trust/School ICT systems unless permission has been given by the Trust CEO/COO or Headteacher.

13 PASSWORDS

For guidance on passwords and management, please see the Cyber **Security** section below**.**

14 CRYPTOGRAPHIC CONTROLS

- All staff laptops must have fully encrypted hard drives
- Removable Disk Media, such as USB Drives, are not permitted to be used on site and a Trust wide policy is in place preventing these from being used.
- Where technology prevents the use of encryption (e.g. memory cards used in Digital Cameras) any personal data must not be stored on these devices.
- Emails sent outside the school network (except for secure portals e.g. Local Authority/DfE), must be encrypted if personal data is being sent. The de-encryption key must not be sent via the same medium as the encrypted data.
- Encryption and RADIUS Authentication is applied to wireless networks throughout the Trust, encryption keys will be kept secure and remain the property of the Central AAT IT Team and must not be shared without permission obtained from the CEO, COO or Headteacher of the school

14 OPERATING SYSTEM PATCHING

- Network security vulnerabilities, missing patches and updates will be monitored and managed by the Central AAT IT Team service daily.
- When it is known that a vulnerability is being actively exploited a patch will be applied immediately and systems will be adjusted and secured accordingly as appropriate.
- Operating systems will be patched and kept updated with the latest releases that are issued.
- Where legacy devices, software, applications and operating systems are in use that are no longer patchable or able to update, therefore becoming a security risk, an upgrade plan for these must be established and in place ASAP.

15 FILTERING

Access to the Internet is filtered using an approved system through our internet service provider. This is managed through our provider and the Central AAT IT Team. Any breaches that occur as a result from filtering, must be reported to a Headteacher and the Trust's Data Protection Officer.

17 EMAIL SECURITY

AAT's requirements for the correct use of emails can be found in the **AAT IT Acceptable Use & Online Safety (Including Online Safety Acceptable Use Agreements) Policy**. Guidance on email security and best practices to follow can be found in the **Cyber Security** section below.

16 INTERNET, SOCIAL MEDIA, E- SAFETY

AAT's requirements for the correct use of internet, and e-safety is outlined within the **AAT IT Acceptable Use & Online Safety (Including Online Safety Acceptable Use Agreements) Policy**.
For guidance on Social Media, this can be found within the **AAT Social Media Policy**.

17 REMOTE WORKING/ACCESS

Remote employees must follow the guidelines within this Policy. Since they will be accessing Trust information and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure. We encourage all staff who work remotely to seek advice from their on-site and the Central IT Team to ensure they are following best practices.

- School data must NOT be stored on any portable or removable ICT device not belonging to a school (including USB memory sticks, cards and hard disks).
- Home working is permitted where authorised by the AAT CEO or Headteacher. The installation of any applications or software packages on school owned portable and mobile devices must only be carried out by your local on-site IT Support Team or the Central AAT IT Team.
- Access to a school's network and school ICT equipment is not permitted to be taken outside the United Kingdom without prior permission from a Headteacher.
- Remote access of the Trust/School's network is strictly prohibited. Measures have been put in place to prevent this and RDP has been retired. The use of software such as TeamViewer, Anydesk, Logmein etc. are also strictly prohibited and not allowed to be installed onto devices.
- All documents and data should be stored and accessed through using Google Workspace/Drive and not through the use of removable disk media, portable storage or mobile devices.

18 ICT SECURITY INCIDENTS

Each school within the Trust has mechanisms in place to properly react and deal with ICT security incidents and violations, both intentional and unintentional. All schools have a current ICT Cyber/Disaster Recovery Plan and procedures in place to follow in the event of such an occurrence taking place.

All ICT security weaknesses and incidents, whether suspected or actual, are to be reported as outlined in the **Trust's Data Protection Policy**. Users must not attempt to prove or exploit a suspected ICT security weakness. ICT security incidents including but not limited to virus attacks, suspicious emails. hardware and software faults, theft or suspected theft of any ICT resources, equipment or information, breach of security resulting in internal fraud or suspected fraud, non-compliance with statutory requirements regarding privacy of information.

19 ICT SECURITY AWARENESS/TRAINING

ICT security awareness mechanisms are in place to ensure anyone who has access to a school's ICT equipment and data are aware of the importance of ICT security, and to properly react and deal with ICT security incidents and weaknesses. User awareness will be supported by regular updates.

- All Staff are required to complete Cyber Security Training for School Staff through the National Cyber Security Centre.
- The Central AAT IT Team will provide and issue Cyber/Security related updates when and where appropriate and necessary.

20 MONITORING

- Users should be aware that the privacy of/in any message, files, data, document, facsimile, telephone conversation, social media post, conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on Trust owned electronic information and communications systems may be subject to monitoring and review.

- The Trust reserves the right to monitor, intercept and review, without prior notification or authorisation from users. For students and BYOD devices, these will be monitored only when in use on the school's network.
- Usage of Trust's IT resources and communications systems activities will be monitored to ensure that Trust rules are being complied with and for the following purposes:
    - to monitor whether the use of school systems and/or the internet is legitimate and in accordance with AAT Policies
    - to assist in the investigation of wrongful and reported misuse
    - to comply with any legal obligation
- Users consent to monitoring by acknowledgement of the Trust's Code of Conduct and the use of Trust resources and systems. The Trust may store copies of data or communications for a period after they are created and may delete such copies from time to time without notice. If necessary, information may be handed to the Police in connection with a criminal investigation.
- Security audit logging is activated on required ICT devices and servers have security audit logging switched on to automatically record events such as failed logon attempts. Critical application systems such as Trust/School MIS and Finance systems will display information and unsuccessful login attempts.
- All Windows servers event logs are checked during regular server maintenance routines.
- The performance of school servers is continually reviewed as part of a regular Server maintenance schedule by the Central AAT IT Team. This includes a review of, but not limited to, system event logs, ICT device/alert messages and disk space.
- CCTV systems monitor school's within the Trust 24 hours a day, this data is recorded and may be used as evidence of any alleged wrongdoing. Please see **AAT CCTV Policy** for more information and guidance regarding CCTV within AAT Schools.
- The Trust reserves the right for appropriately elected employees to use approved software tools to monitor school network, systems and emails in order to check compliance with this and other AAT IT Policies. This will be authorised by the CEO and/or Headteacher.

21 DISCIPLINARY ACTION

Disciplinary action may be taken against any User suspected of being in breach of this Policy, including an immediate ban from using the school's ICT facilities and equipment. Breaches of this Policy may constitute gross misconduct and as such may lead to staff dismissal. For individuals not directly employed by the Trust, breaches of the Policy may result in withdrawal of facilities, rights and immediate access removal. For all other users, a breach of this Policy may constitute a breach of the Code of Conduct and may lead to sanctions being applied and further actions taken if deemed necessary.

The Police will be informed where there is a possibility that a criminal offence has been committed.
If an employee is aggrieved or wishes to register or report a complaint, they must follow the Trust's Whistleblowing Policy and/or Staff Grievance Procedures.

CYBER SECURITY

This section covers Alban Academies Trust's approach to our Cyber Security guidelines and provisions for preserving the security of our ICT, data and technology infrastructure. As we become ever more reliant on technology to collect, store and manage information, the more vulnerable and open we are to severe security breaches. Elements including human error, hacker attacks and system malfunctions can cause catastrophic financial damage and can put at risk the Trust's reputation. For this reason, AAT have implemented the following security measures and have developed clear and concise instructions to help mitigate security risks.

Correct Cyber Security approaches apply to all AAT employees, contractors, volunteers and any individual associated who has permanent or temporary access to our systems and hardware.

1. ELEMENTS

CONFIDENTIAL DATA

Confidential data is information that allows public identification, which might cause harm to a respondent or establishment if released. Common examples are:

- Personal information relating to staff, students, parents, governors and partners.
- Financial information
- Sensitive and contractual data

All employees are obliged and responsible to protect confidential data. This **AAT ICT & Cyber Security Policy** will outline and give guidance to all AAT Staff, on how to avoid security breaches and the best security measures to follow in relation to this.

PROTECTING PERSONAL AND TRUST DEVICES

When AAT Staff use their devices to access Trust/School emails or accounts, there is a security risk introduced to our data. We advise and recommend all AAT employees and students to keep both their personal and Trust devices secure at all times. This can be achieved by:

- Ensuring all devices are password protected
- Ensuring antivirus on your devices is kept up to date.
- Ensuring devices are kept safe, secure and never left unattended
- Ensuring devices are securely locked away when possible or left with IT if this is not possible
- Installing all security updates when prompted or as soon as updates are available.
- Contacting and reporting to IT any concerns or suspicious activity
- Log into company accounts and systems through secure and private networks only.

All AAT employees and students must not access internal systems and accounts from other people's devices and the lending of their personal devices to others.
When AAT Staff receive Trust equipment they should review the **AAT IT Acceptable Use & Online Safety (Including Online Safety Acceptable Use Agreements) Policy**, this Policy contains key information relating to the safe and secure use of equipment and guidance to follow regarding this.

EMAILS

Emails are often open to phishing attacks, scams or malicious software. To avoid the risk of these types of potential virus infections or data thefts, we advise all AAT employees and students to carefully follow the below steps:

- Avoid opening emails and attachments from unknown senders
- Be cautious of emails threatening to block, remove or requesting information
- Avoid opening emails and attachments from suspicious looking email addresses, for instance ***"@office365protectionservices.com"***
- Avoid opening attachments and clicking on links where content is not adequately explained, for instance ***"Click Here Now!"***
- Be suspicious of clickbait titles, offering prizes or to claim your winnings
- Check email addresses and names of people carefully to ensure the sender is legitimate
- Look for general inconsistencies and obvious indications such as: grammatical mistakes, inconsistent capital letters, excessive number of exclamation marks.) If an employee isn't sure that an email they have received is safe, they should contact their on-site IT Support Team or the Central AAT IT Team.

If you receive an email that you believe is suspicious or of concern, please contact or see the on-site IT Support Team or the Central AAT IT Team. Never attempt to open or deal with this yourself, IT will resolve and provide guidance and advice for all AAT Staff and Students. It is vital to remember, when it comes to Cyber Security, no question is ever regarded as trivial. It is always considered best practice to report any uncertainty over emails to a member of IT.

PASSWORD MANAGEMENT

Password leaks are incredibly dangerous, a single incident of password exposure can compromise and bring down the entire AAT infrastructure. It is imperative that passwords are not only secure to prevent them from being easily hacked, but they should also remain confidential and never shared. We ensure that all AAT Staff and Students have and follow:

- Passwords with the following rules and combination: eight characters minimum, including capital, lower-case letters and numbers.
- Remember passwords instead of writing them down. In the instance that passwords need to be written, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Never exchange or share passwords with anyone outside of IT. If requested by IT, this should be shared in person or over the phone, never over email.
- As per AAT policy, passwords are to be changed every 90 days to ensure a high level of security and that best password practice is adhered to.
- System administrator passwords are kept in a secure and protected location with permissions and rights only to those requiring access.
- Administrative passwords will be immediately changed when a member of the school’s ICT team or anyone who has access rights leaves.

TRANSFERRING OF DATA

The transfer of data involves a security risk. To reduce this, employees must:

- Avoid transferring sensitive data (e.g., student information, employee records) to other devices or accounts unless absolutely necessary and permission has been given from IT. When mass transfer of such data is needed, we request employees seek the support of their on-site IT Support or the AAT Central IT Team for help.
- Only ever share confidential data over the company network/system and ***never*** over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised and/or organisations that have adequate security policies.
- Report scams, privacy breaches and hacking attempts. Your on-site IT Support and Central IT Teams need to be made aware about scams, breaches and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible.
- In the event of the above, the IT Team will investigate promptly, resolve the issue and send a Trust-wide or school alert when necessary.
- Your on-site IT support and the Central AAT IT Team are responsible for advising employees on how to handle and proceed with the above. We encourage our employees to reach out to them with any questions or concerns and report anything, however minor it may appear, to IT if there are any concerns over anything.

ADDITIONAL MEASURES

To reduce the likelihood of security breaches, we also instruct all AAT staff to:

- Turn off their screens and lock their devices when leaving their desks.
- Report stolen or damaged equipment as soon as possible to on site or Central IT Teams.
- Change all account passwords immediately if a device is stolen.
- Report a perceived threat or possible security weakness in school systems.
- Refrain from downloading suspicious, unauthorised or illegal software on their Trust equipment.
- Avoid accessing suspicious websites.
- We also expect our employees to comply with all AAT IT policies.

Your Local and Central IT Team will:

- Manage and keep the Trust’s Network and infrastructure secure
- Arrange for security training to all employees as part of initial induction for new joiners and annually for existing staff.

- Inform employees regularly about potential threats and security concerns.
- Investigate instances of security breaches, security concerns and reports thoroughly.
- Alban Academies Trust will have physical and digital shields to protect information.

3. IMPORTANCE OF SECURITY

Everyone should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and data. We can all contribute to this by being vigilant and keeping cyber security at the top of our minds.

4. SAFEGUARDING

Schools have a statutory duty to monitor their digital environment to identify any potential threats to pupils' welfare and wellbeing. AAT have appropriate filtering and monitoring tools in place and have the right to monitor all devices and activity when and where necessary. For student owned devices, this monitoring will only take place when on the internal school network.

5. CYBER ATTACK & DATA BREACHES

In the event of Alban Academies Trust or one of its schools experiencing a cyber attack then the AAT Director of IT alongside relevant parties will action the Cyber Response Plan/s that are in place for each setting. Due to the confidential content of these documents, these plans are kept and held securely by the central AAT IT Team.

If Alban Academies Trust or one of its schools experience a data breach, then the Data Breach Response Plan will be enacted, details of which can be found within the **Data Protection and Data Breach Response Plan**.

In the event of a cyber attack and/or data breach impacting examinations, then the **Exam Cyber Response Plan** (see ***Appendix A***) will be actioned in conjunction with the School's Cyber Response Plan.

6. REPORTING & CONTACT DETAILS

Any questions or reports relating to this policy should be addressed to:

Luke Harman
AAT Director of IT
harmanl@albanacademiestrust.org.uk

James Belmont
AAT Digital Infrastructure Lead
belmontj@albanacademiestrust.org.uk

Mark Allday
AAT Director of Digital Strategy and Innovation
alldaym@albanacademiestrust.org.uk

7. REVIEW

This policy will be reviewed on an annual basis.

APPENDIX A - Exam Cyber Attack Response Plan

Alban Academies Trust takes the potential threat of a Cyber Attack very seriously and as a school, we have a Response Plan set out with our Insurer for each individual school within the Trust.

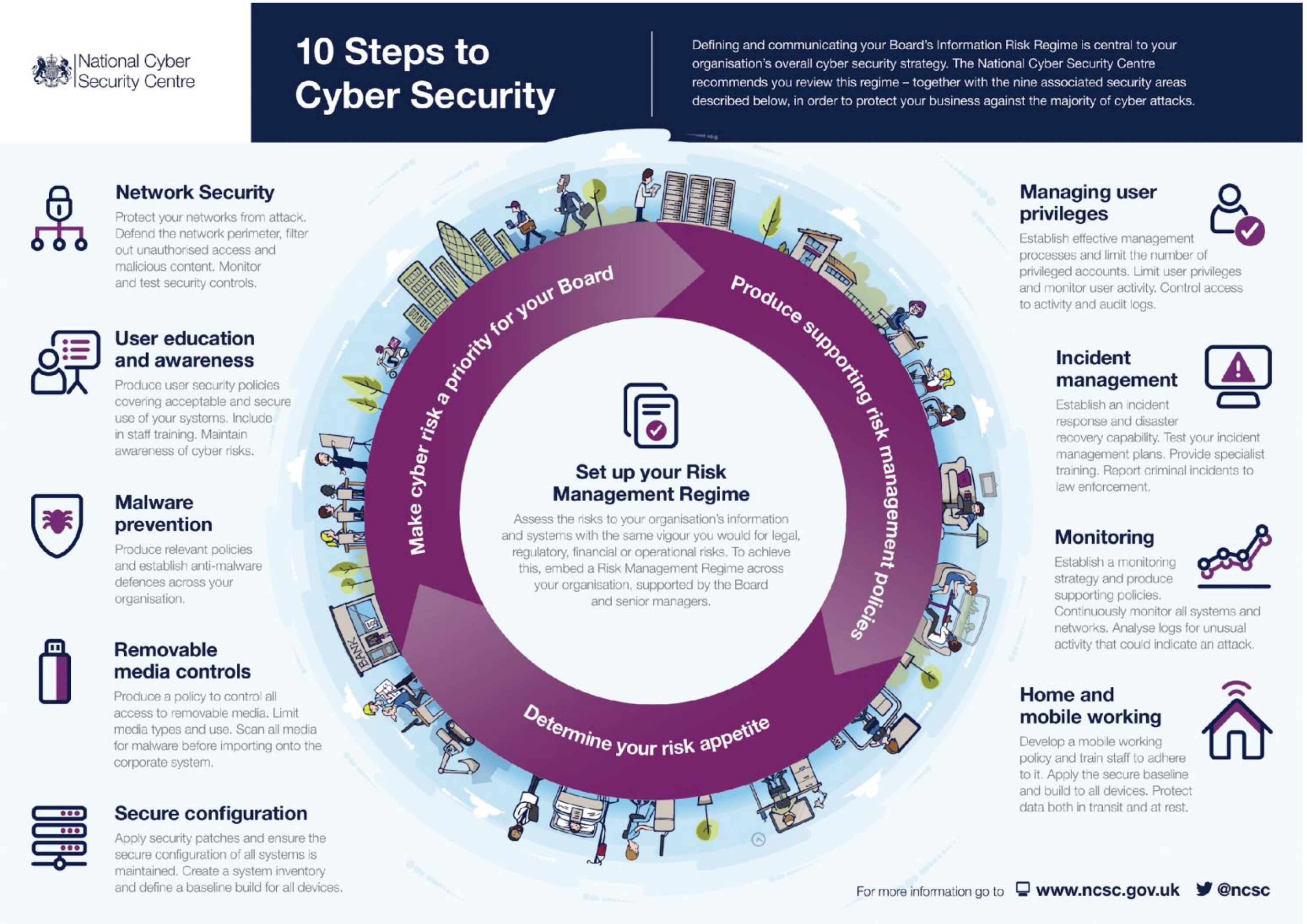
This Exam Cyber Attack Response Plan details the specifics related to exams taking place over Summer 2023 and should be only actioned in conjunction with the School's Cyber Response Plan.

Further advice has been provided by JCQ, which can be found here:

https://www.jcq.org.uk/dfe-and-national-cyber-security-centre-ransomware-update/

Access Issues Preventing Continuity Of Exam Process	Time Impact	Impact Level	Possible Work Solutions & Data Required
Access To Exam Site & Official Documentation	1 Week	Medium	
Access To Exam & Controlled Assessment Entries	1 Day	Medium/High	
Access To Pupil Data Concerning Special Considerations	1 Week	Medium	
Access To Exam Payment Services	1 Month	Low	
Administration Of Ongoing Exams (Timetabling, Organising Resources And Submitting Paperwork)	1 Week	Medium	
Access To Contact Details Of Invigilation Staff	1 Month	Low	

APPENDIX B - NCSC 10 Steps To Cyber Securit



National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Make cyber risk a priority for your Board

Produce supporting risk management policies

Determine your risk appetite

Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc