IMPACT
Multi Academy Trust

Cyber-Security Policy

Owner (Job Role):	COO
Approval Body:	Resources and Finance Committee
Approval Date:	Operational Revision of Policy – For Approval in December 2025
Implementation Date:	November 2025 (As operational policy)
Review Date:	December 2026
Related Policies:	Acceptable Use of Technology Policy Online Safety Policy Data Protection Policy (See section 18 for full listing)

Version	Approval Date	Summary of Changes
1	October 2025	Original Version of Policy (Operational, pre board approval)

Inspire, Respect, Flourish.

Contents

Our Vision and Values 4

0. Introduction 4

1. Legislation and External Guidance 5

2. Scope and Responsibilities 5

3. Detailed Roles and Responsibilities 6

Trustees 6

Trust Senior Central Team 6

School Local Governing Body (LGB) 6

Headteachers 6

All Staff 6

IT Support Staff 6

Pupils 7

Parents/Carers 7

4. Risk Management 7

5. Major Incident Response Plan 7

6. Physical Security 7

7. Asset Management 8

8. User Accounts and Management 8

9. Devices 9

Device Imaging 10

10. USB Drives 10

11. Data Security 10

Immutable Backups 10

Offline Tape Backups 10

Cloud Based Backup 11

Cloud Hosting 11

12. Email Security 11

13. Sharing Files and Data 12

14. Staff Training and Awareness 12

15. System Security 12

16. Maintaining Security 13

17. Review and Updates 13

18. Links with Other Policies 13

Appendix 1: Types of Cyber-security Attacks 14

Cybercriminals and Cybercrime 14
Hacktivism.......... 14
Insiders.......... 14
Zero-day Exploit 14
Appendix 2: Additional Information Regarding Examination Staff and Services 15

Our Vision and Values

Our Vision
Together, we enable everyone to thrive.

Our Values

- Ambition – we have high aspirations for our children and strive to do our very best.
- Inclusion – we care about the whole child, and everyone will feel that our Trust is a place where they are valued, respected, safe and happy.
- Collaboration – we are stronger together and collaborate generously to ensure the long-term success of our children, our staff, our schools and the communities we serve.
- Trust – we build trust by acting with integrity and kindness and by putting children first.

Inspire, Respect, Flourish.

0. Introduction

A cyber-security incident is an attack launched from one or more computers against another computer or network of computers. It can maliciously deactivate computers, steal or encrypt data, or use a compromised computer as a launch point to further deploy the attack.

The aim of a cyber-security attack is to either disable the system or gain illegal access to the target computer or network. There are different types of cyber security attacks based on their specific method and intention. A cyber-security attack is a malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation. Usually, the attacker seeks some type of benefit from disrupting the victim's network.

A cyber-security incident can have a major impact on any organisation for extended periods of time. For a school, this can range from minor reputational damage and the cost of restoring systems from existing backups, to major incidents such as losing student work or access to learning platforms and safeguarding systems, which could lead to data-protection fines or even failing an inspection.

In the past few years, the National Cyber Security Centre has issued several alerts to schools, warning of an increase of malware attacks, in particular ransomware, targeting educational establishments. A number of schools have been forced to pay the ransomware attackers so that they can recover their data. The complexity and variety of cyber-security attacks is ever increasing. While cyber-security prevention measures differ for each type of attack, good security practices and basic IT hygiene are generally good at mitigating these attacks.

In addition to implementing good cyber-security practices, we are advised to keep systems and security software up to date, leverage firewalls, threat management tools and solutions, install antivirus software across systems, control access and user privileges, backup systems often, and proactively watch for breached systems.

The purpose of this policy is to highlight the potential cyber-security risks to the Trust, making clear what we currently have in place to prevent such events occurring, and to highlight what is regarded as the basic principles of good cyber-security, protecting our systems, services and data in the event of a cyber-attack.

1. Legislation and External Guidance

This policy reflects good practice guidelines/recommendations in the following publications.

Department for Education (DfE), Ofqual, Ofsted:

- Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK

National Cyber Security Centre:

- Cloud security guidance - NCSC.GOV.UK
- Cyber security advice for public sector organisations - NCSC.GOV.UK

JCQ:

- General Regulations for Approved Centres - Joint Council for Qualifications

Data Protection Regulation:

- The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Data Protection Act 2018 (DPA 2018)
- UK General Data Protection Regulation (UK GDPR)

Other Useful Links:

- Security - LGFL
- BCS, The Chartered Institute for IT | BCS
- Microsoft – Cyber Security Awareness

2. Scope and Responsibilities

This policy applies to all members of our school community, including pupils, teachers, administrative staff, governors and anyone else granted permanent or temporary access to our systems and hardware. It also covers the physical and technical elements that are used to deliver IT services for the Trust.

All staff are responsible for reading and understanding this policy. All leaders are responsible for ensuring their staff read and understand this policy and that they follow this policy, including reporting any suspected breaches of it.

For the purposes of clarity, “IMAT” or the “Trust” in this document can be used as shorthand to refer to the individual schools in the Trust or the broader Trust as a whole.

For the purposes of clarity, “Users” in this document can be used as shorthand to refer to staff, students, contractors, volunteers and anyone else granted permanent or temporary access to our systems and hardware.

3. Detailed Roles and Responsibilities

Trustees

- Approve and adopt the cyber-security policy
- Ensure the policy is reviewed and updated regularly
- Review annual reports on cyber-security implementation effectiveness, policy compliance and to assess risk

Trust Senior Central Team

- To lead on matters of cyber-security, producing policy and approving and implementing controls and requirements
- To oversee and lead the IT Support teams
- Allocate resources for cyber-security implementation, training, and infrastructure
- Report to Trustees on cyber-security implementation progress and challenges

School Local Governing Body (LGB)

- Monitor policy implementation and ensure sufficient resource is allocated (i.e., in budgets) for cyber-security implementation, training, and infrastructure at local school level

Headteachers

- Support the Senior Central Team, leading within schools to implement the cyber-security policy
- Establish a culture of responsible use of technology
- Ensure staff are appropriately trained with regards to cyber-security, in line with trust mandatory training requirements
- Immediately escalate any concerns about major cyber-security issues/threats to the COO or Trust Technology Officer

All Staff

- Use technology responsibly in accordance with trust/school policies
- Participate in technology and cyber-security-related professional development
- Report any concerns about cyber-security

IT Support Staff

- Maintain the technical infrastructure to maintain high cyber-security standards
- Support staff and pupils with technology to maintain high cyber-security standards
- Implement security measures
- Monitor network usage related to security risks

- Stay informed about technical developments in cyber-security
- Immediately escalate any concerns about major cyber-security issues/threats to the COO or Trust Technology Lead

Pupils

- Use technology responsibly in accordance with the school policy and teacher guidance
- Report any concerns about cyber-security

Parents/Carers

- Support the trust's approach to cyber-security
- Communicate with the school about any concerns regarding cyber-security
- Stay informed about the school's cyber-security policies and practices

4. Risk Management

IMAT will include cyber-security risks on its organisational risk register, regularly reporting on the progress and management of these risks to Trustees 3 times a year.

5. Major Incident Response Plan

IMAT develops, maintains, and regularly tests our Cyber-security Major Incident Response Plan. This includes the following:

- Steps for identifying and reporting incidents
- Key decision-makers and the incident response team
- Communication plan for stakeholders
- Key system impact assessments and restoration priorities (i.e. which backups needs to be restored first for the Trust or school to become operational again)
- Emergency plans for the Trust or school to function without access to systems or data
- Alternative methods of communication, including copies of contact details
- Emergency budgets and who can access them / how
- Key agencies for support (e.g. IT support company)
- Post-incident review process: Conducting a review to identify lessons learned and update procedures if necessary.

Due to the sensitive nature of the content contained within the Plan, the plan is not published publicly but is available to the relevant members of staff.

6. Physical Security

The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster, natural or otherwise, that impacts upon IT systems. These can impact cyber-security and are considered part of physical security risks or environmental threats in the broader context of information security.

IMAT will ensure there is appropriate physical security and environmental controls protecting access to its IT Systems, including but not limited to air conditioning, lockable cabinets, temperature monitoring, and secure server/communications rooms.

7. Asset Management

To ensure that security controls to protect the data and systems are applied effectively, IMAT 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.

8. User Accounts and Management

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they will not be easily hacked, but they should also remain secret.

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised, for example after a suspected phishing scam, they must change their password and inform the IT Support team as soon as possible. Personal accounts should not be used for work purposes.

We advise all Users to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers, and symbols) and avoid information that can be easily guessed (e.g., birthdays). A good way to make a password difficult to crack is by combining three random words to create a password (for example AppleNemoBiro). NCSC Top Tips for Staying Secure – Three Random Words
- Remember passwords instead of writing them down. If a User needs to write down a password, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Never share credentials with other Users
- Change all account passwords immediately if a device is stolen
- Do not use the same password for different systems, services or platforms. Passwords should be unique.

IMAT will implement multi-factor authentication (MFA, also known as 2FA) where it is practicable to do so, and Staff are expected to implement such security measures where available on systems not directly provided by IMAT.

IMAT takes the approach of "Principle of Least Privilege", providing all Users the lowest access required for them to undertake their daily tasks. Staff and Students are Standard Accounts on IMAT issued devices, lowering the risk of malware running unhindered on a device with a high level of privilege. IT Support staff have Standard Accounts for their day-to-day tasks, and a separate account dedicated to performing higher administrative functions.

Access control and permissions are based on job roles and reviewed regularly; IMAT ensures file and folder permissions allow access only to those people who need it, for example to financial information, allowing control of who can edit and delete files on network shares or SharePoint.

Whilst this is not a guarantee of protection, as vulnerabilities exist in operating systems that allow attackers to promote themselves to administrator level, it does lower the risk of this happening.
In addition, IT Support staff will ensure that accounts are promptly disabled when Users leave, and account activity is monitored and audited.

9. Devices

To ensure the security of all IMAT issued devices and data, IMAT issued devices will be configured with the following security controls as a minimum:

- Password protection
- Full disk encryption
- Client firewalls
- Anti-virus / malware software
- Automatic security updates
- Removal of unrequired and unsupported software
- Autorun disabled
- Minimal administrative accounts

To ensure the security of all IMAT issued devices and data, Users are required to:

- Keep all devices password protected.
- Ensure they do not leave their devices exposed or unattended.
- Lock their devices when leaving their desks
- Update devices if/when prompted
- Report stolen or damaged equipment as soon as possible to the IT Support team
- Change all account passwords immediately if a device is lost or stolen and report the loss immediately to the IT Support team.
- Log into IMAT accounts and systems through secure and private networks only (not public/insecure Wi-Fi connections).
- Report a suspected threat or security weakness in IMAT systems to the Trust IT Manager, Trust Technology Officer or COO.

When Staff receive IMAT issued devices they should review the Acceptable Use Policy, as it will contain key information relating to the safe and secure use of this equipment.

When staff use their personal (also called Bring Your Own Device - BYOD) to access IMAT systems, they introduce a security risk to our data. We advise staff to keep both their personal and IMAT issued devices secure. They should do this by:

- Ensuring antivirus/antimalware software is kept up to date.
- Installing security updates of browsers and systems monthly or as soon as updates are available.

We also advise Users not to access IMAT systems and accounts from other people’s devices or lending their own devices to others.

Device Imaging

IMAT schools leverage Windows Deployment Services (WDS) or the Microsoft Deployment Toolkit (MDT) to deploy the base operating system and applications as applicable (the “image”). This would allow us to re-image any infected computers (excluding servers) to get systems back up and running. To ensure that we have access to images in the event that the WDS/MDT server itself is attacked, IMAT keeps a set of images on external media.

10. USB Drives

Users are generally prevented from using USB memory sticks or external hard drives on IMAT issued devices, allowing us to mitigate the risk of malware being brought into IMAT systems via these devices.

In some situations, attackers have been known to leave infected USB memory sticks in staff car parks in the hope that someone will pick up the infected memory stick, insert it into their work computer, and then provide an attacker with a way into the device from there. If a staff member finds a USB memory stick anywhere, they should pass the found item to IT Support.

11. Data Security

IMAT will take appropriate measures to reduce the likelihood of the loss of availability to, or the disclosure of, confidential data.

IMAT defines confidential data as:

- Personally identifiable information as defined by the ICO
- Special Category personal data as defined by the ICO
- Unpublished financial information
- Sensitive operational information

Critical data and systems will be backed up on a regular basis following the 3-2-1 backup methodology

- 3 versions of data
- 2 different types of media
- 1 copy offsite/offline

IMAT’s backup strategy allows for the backup and restoration of the entire environment as well as file level backup and restoration of the storage area file servers.

Immutable Backups

IMAT uses backup solutions with immutability. Immutable backups cannot be modified, deleted, or overwritten, ensuring data integrity and security. They are effective in protecting against ransomware attacks, as they provide a clean, unaltered copy of data that can be recovered quickly.

Offline Tape Backups

One of the most secure ways of restoring from a ransomware attack is to use offline backups that have been unaffected by the attack. Once the network is deemed safe to restore, the offline tape backups can be utilised if other backup media have been compromised. However, due to the speed of performing tape-based backups the age of the data on these backups may be significant. Due to the time constraints between backup jobs, it would not be possible to keep continuous weekly tape backups without impacting upon the regular disk-based backup routines.

Cloud Based Backup

As part of the Shared Responsibility Model, Microsoft's responsibilities for Microsoft 365 relate to backend infrastructure and providing service delivery resiliency so there is little to no service interruption. Responsibility for the data remains with the customer.

Whilst Microsoft 365 is separate to a School's internal network infrastructure, it is still vulnerable to encryption of data by way of a user syncing encrypted data to Microsoft 365. In order to mitigate the risk of user data being unrecoverable from Microsoft 365's own data retention and restoration abilities, IMAT utilises a cloud-based backup service, allowing the backup of Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams. This gives us the ability to restore the above-mentioned data even if the synchronised versions are encrypted.

In addition to the above, Microsoft OneDrive allows for 30 days of point in time restoration of a User's OneDrive storage area. This allows for restoration in the case of their device synchronising any encrypted data back up to OneDrive.

Cloud Hosting

As a method of protection, keeping data in a cloud environment offers a robust and secure method of protection. The Trust MIS is Bromcom, whose MIS and apps are hosted on Microsoft Azure, making them secure and accessible from online devices. If an attack did occur at a School, MIS data is accessible to the staff via any Internet connection and unaffected device.

12. Email Security

Emails often host phishing attacks, scams, or malicious software (e.g., trojans and worms.) IMAT uses Microsoft 365 email protection which allows us control over our email system and provides anti-spam tools to help stop attacks before they reach the user mailboxes. Compulsory aged student accounts are not allowed to email externally or receive emails from external sources unless otherwise whitelisted (for example, to receive a password reset email for an online University service).

To avoid virus infection or data theft, we instruct Users to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g., "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g., offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.)

If a User is not sure that an email they receive is safe, they should contact the IT Support Team.

13. Sharing Files and Data

IMAT recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a date breach, Users are required to:

- Avoid transferring sensitive data to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we advise staff contact the IT Support team.
- Share confidential data via the IMAT network/system and not over public Wi-Fi or private connection.
- Consider if an email could be a phishing email or that a colleague's account could be 'hacked'. If something does not feel right check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites
- Keep IMAT's files within the Trust's Microsoft 365 ecosystem, on IMAT servers, approved platforms or on encrypted Trust issued devices. Never store data on systems or platforms not approved for use by the Trust.
- Not send IMAT files/data to personal accounts.
- Verify the recipient of data prior to sending and ensuring that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Use file encryption where possible, sending passwords/keys via alternative communication channels
- Alert the DPO of any breaches, malicious activity or suspected scams

14. Staff Training and Awareness

IMAT recognises that it is not possible to maintain a high level of cyber-security without appropriate staff training. It will integrate regular cyber-security training into Inset days and promote a "No Blame" culture towards individuals who may fall victim to sophisticated scams.

All Staff must complete annual cyber-security training. This is to ensure that staff are kept informed of existing and emerging threats posed by cyber-security attacks. Annual training of all staff is a requirement of the RPA cyber-attack coverage.

Training will be sent out electronically and is recorded centrally to allow for inspection of training records.

15. System Security

IMAT integrates security principles into the design of its IT services.

- Regular software and security updates – network hardware, operating systems and software
  - As part of our maintenance plans, IMAT endeavours to keep all our servers and client devices on the latest releases of Microsoft, Apple, Linux or 3rd party appliance security releases. This allows us to mitigate the risk of an attacker using known exploits in systems to gain elevated privileges on the IMAT network. Updates on User devices are managed and controlled by IT support to ensure essential updates are installed in a timely manner.
- 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 and anti-malware systems
    - Sophos Intercept X is our primary anti-virus/anti-malware tool which helps with the prevention of ransomware attacks. We utilise a secondary system in Microsoft Endpoint/Defender Protection. The software is to be installed on all client and server devices and actively monitors all file and executable activities on the device. When Intercept X detects that a file is being encrypted, it immediately shuts down the process and quarantines the affected files and processes involved, therefore helping prevent the spread of the attack. Intercept X also has methods of control that prevent it from being shut down by an attacker before the malware starts encrypting data.
- Actively manage and test backups
- Actively manage firewalls and network security controls
- Encryption for sensitive and personal data
- Regularly review and update security controls that are available with existing systems, including for Microsoft 365
- Segregate wireless networks used for visitors' and staff personal devices from school systems
- Review the security risk of new systems or projects, including GDPR assessments
- Prompt removal of access for leavers.

To reduce the likelihood of security breaches, we also instruct Users to:

- Report a perceived threat or possible security weakness in IMAT systems.
- Refrain from downloading suspicious, unauthorised, or illegal software on their IMAT issued devices.
- Avoid accessing suspicious websites.

16. Maintaining Security

IMAT understands that the financial cost of recovering from a major cyber-security incident can far outweigh the ongoing investment in maintaining secure IT systems. IMAT will budget appropriately to keep cyber related risk to a minimum.

17. Review and Updates

This policy will be reviewed and updated **annually**, to keep pace with the rapidly evolving cyber-security landscape.

18. Links with Other Policies

This Cyber-security policy is linked to our:

- Trust Data Protection Policy
- Trust Acceptable Use (AUP) Policies
- Trust Online Safety Policy
- Trust Bring Your Own Device (BYOD) Policy
- Trust Records Management (Retention) Policy

- Trust Privacy Notices

Appendix 1: Types of Cyber-security Attacks

The following list highlights some common examples, though it is not comprehensive.

Cybercriminals and Cybercrime

Cybercriminals are generally working for financial gain. Most commonly, for the purposes of fraud: either selling illegally gained information to a third party or using directly for criminal means.
Key tools and methods used by cybercriminals include:

- Malware – malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals
- Ransomware – a kind of malware that locks victims out of their data or systems and only allows access once money is paid
- Phishing – emails purporting to come from a public agency to extract sensitive information from members of the public.

Hacktivism

Hacktivists will generally take over public websites or social media accounts to raise the profile of a particular cause. When targeted against local government or trust/school websites and networks, these attacks can cause reputational damage locally. If online services are regularly disrupted by cyber-attacks this could lead to the erosion of public confidence in using such services. Hacktivist groups have successfully used Distributed Denial of Service (DDoS – when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable) attacks to disrupt the websites of several schools already.

Insiders

Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party but often is due to simple human error or a lack of awareness about the risks involved.

Zero-day Exploit

A zero-day exploit refers to a cyber-attack that is initiated on the same day a vulnerability is identified within software or firmware. This type of exploit takes advantage of security flaws before the developer has released an appropriate update or patch. By targeting previously undiscovered vulnerabilities, zero-day exploits present significant risks to computers and systems that have not yet received relevant updates or antivirus protection.

Appendix 2: Additional Information Regarding Examination Staff and Services

Due to the sensitive nature of the data provided to users accessing awarding bodies' online systems, it is imperative that staff who have access to these systems adequately secure their accounts to reduce the risk of a cyber or GDPR breach. This can be achieved through the use of Multifactor Authentication where it has been made available for use.

Staff should refer to the table below detailing MFA support, which was accurate upon date of publication. For those which do not currently support MFA, staff should check for updated guidance from the examining body.

Examining Body	MFA Support
AQA (Assessment and Qualifications Alliance)	Yes
CCEA (Council for the Curriculum, Examinations & Assessment)	None specified
City & Guilds	City & Guilds are rolling out MFA with the plan to finish implementation in 2026. Codes will be sent via Email. Support from City & Guilds: MFA
Edexcel (Pearson)	Yes – Pearson Portal Authenticator Support from Pearson: Pearson Portal Authenticator
NCFE (Northern Council for Further Education)	None specified
OCR (Oxford Cambridge and RSA Examinations)	Yes – Authenticator App (Google Authenticator, Microsoft Authenticator) Support from Cambridge OCR: Setting up MFA
SQA (Scottish Qualifications Authority)	None specified
WJEC (Welsh Joint Education Committee)	Yes – Authenticator App (Google Authenticator, Microsoft Authenticator), Text Message, Email Support from WJEC: Portal Quick Guide

Further detail regarding the operation of examinations in relation to IT systems and services can be found within individual school examination policies.