



INFORMATION SECURITY POLICY

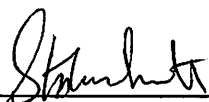
CHANGE CONTROL

<i>Date</i>	<i>Issue</i>	<i>Details of change</i>
01.07.2017	0.a	Initial Draft
18.10.2017	1.0	Changes agreed and policy approved at Trust Board Meeting on 17 th October 2017
November 2019	1.a	Amendments to policy made
27.11.2019	2.0	Changes agreed and policy approved at Trust Board Meeting on 27 th November 2019
22.06.2021	2.a	Policy updated following review
30.06.2021	3.0	Policy updated following Board Approval at meeting on 30.06.2021
Summer 2023	3.a	Policy updated following review
Summer 2023	4.0	Policy updated following Board Approval at meeting on 14.06.2023

AUTHORISATION

Approved at Board Meeting held on 14th June 2023

Signed:



14-6-23

Chair of Board

Date

INSIGHT MAT POLICIES AND PROCEDURES

This policy pertains to all employees and, as appropriate, Governors, Trustees, Members, contractors, visitors and volunteers connected to Insight Multi-Academy Trust (IMAT).

1. Introduction

1.1 The **Information Security Policy** is the overarching information security management policy of IMAT which includes the policies and other documents listed below:

- Acceptable Use Policy
- Data Protection Policy
- Freedom of Information Policy
- Records Management Policy
- Staff Code of Conduct
- Safeguarding Policy
- Student Code of Conduct
- Complaints Policy
- E-safety Policy

1.2 The Trust has a duty to ensure that information is correctly and professionally managed in the interests of:

- Confidentiality
- Integrity
- Availability

2. Aim

2.1 The aim of this policy is to provide a documented record of requirements for Information Assurance.

2.2 IMAT is responsible for all data and information collected, analysed, stored, communicated and reported, and protecting it from theft, misuse, loss and corruption.

2.3 This policy is intended to create an environment in which data and information is. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

3. Key Elements

Scope

3.1 This policy applies to:

- all constituent academies and services in IMAT
- all permanent and temporary employees, working at all locations, including those working from home
- other workers (e.g. casual and agency workers, secondees, volunteers and contractors) provided with access to the Trust's equipment, systems or information used for Trust purposes
- Local Governing Body Governors
- Trustees and Members of the Trust Board.
(together the "Users").

Policy Statement

- 3.2 IMAT is committed to the protection of information and administrative resources, including paper and electronic resources and the media in which they are stored or transmitted.
- 3.3 IMAT will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed. See **Records Management Policy** for details.
- 3.5 IMAT will make every effort to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- 3.6 IMAT will ensure all personal data is obtained fairly in accordance with the "Privacy Notices" and lawfully processed – See **Data Protection Policy**.
- 3.7 To ensure confidentiality, information will be protected against unauthorised access and only authorised personnel will modify it. See **Records Management Policy** for details.
- 3.8 Security measures such as encryption and password protection for electronic media, and secure storage for hard copy material will be provided to protect against theft or loss.
- 3.9 Staff will receive training and guidance at INSET days, Staff Meetings and dedicated sessions to enable them to understand, and appropriately apply, security measures for the protection of all information.

INSIGHT MAT POLICIES AND PROCEDURES

- 3.10 Regulatory and legislative requirements as included within the Data Protection Act 2018, General Data Protection Regulations (GDPR), the Freedom of Information Act 2000, and the Education (Pupil Information) (England) Regulations 2005 will be met. This may include sharing personal data where it is fair and lawful to do so.
- 3.11 The Headteacher is the Senior Information Risk Owner for their respective academy and has day to day responsibility for managing information security within their academy. The Headteacher may delegate to named 'Responsible Officers' in the academy.
- 3.12 The Chief Executive Officer is the overall Information Risk Owner and has responsibility for the implementation of this policy and the management of information security across IMAT.
- 3.13 The Chief Financial Officer has overall responsibility for maintaining this policy and the operational guidance and providing advice and guidance on implementation.
- 3.14 The individual Academy Headteachers and academy Business Managers will conduct initial Information Asset audits and subsequent reviews to identify the full range of information assets and Information Asset Owners in each academy (see **Appendix 1**).
- 3.15 Staff are responsible for adhering to this policy and implementing the policy in their areas of responsibility.
- 3.16 This policy and the accompanying guidance will be reviewed, and if necessary updated, biennially or sooner if legislation changes or an incident arises.

Operational Guidance for IMAT Academies

Security and care of equipment

- 3.17 All items of equipment are the property of the Trust and as such must be kept well maintained and secure at all times.
- 3.18 If a member of staff wishes to borrow a piece of academy/departmental equipment, (a laptop, camera etc) full details will be recorded by the ICT Team or the HOF or Line Manager using the Equipment Loan Form included in **Appendix 3**. Teacher laptops will be issued by the ICT Team on Form included as **Appendix 4** setting out expectations and relevant policy documents and these must be reviewed and signed annually.
- 3.19 If the equipment is lost or stolen the Headteacher must be notified in the first instance and will decide on the appropriate course of action which may include

notifying the Police. If any data is compromised the process set out in **Appendix 2** must be followed.

- 3.20 If equipment is being used for processing personal data then the procedures given below (Security of data) should be followed to ensure the data was kept safe from disclosure.
- 3.21 All equipment will be proprietorially marked using an approved security marker to aid identification if recovered, following theft or loss. An asset register which lists all equipment will be kept by the academy – this should include a list of identifying information such as equipment ID's.

Security of data

- 3.22 IMAT has a statutory duty under the Data Protection Act 2018 and GDPR to ensure appropriate technical and organisational measures are taken to protect personal data against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- 3.23 All staff should ensure that any electronic or paper documents which contain personal data or, are otherwise confidential, are protected against unauthorised access. This includes ensuring that paper records are securely locked away, not just at the end of the day but when staff are out of the office, and that staff operate a clear desk policy and lock screens when away from their desks.
- 3.24 Computers should be password protected. Any personal or academy provided memory sticks or removable devices used to store personal data, or used by staff away from the academy, must be password protected and encrypted, although staff are advised to use Office 365 to store information rather than removable devices. Staff **MUST NOT** use private equipment to store personal data and must seek advice from the Headteacher if there is a need to do so.
- 3.25 Staff must ensure that they have read, understood and signed the **Acceptable Use Policy** which sets out the details of their responsibilities in relation to electronically held data and information.
- 3.26 Servers and back-up systems should be kept securely in locked cabinets or a locked area to which only named staff have access.
- 3.27 Use of emails and scanners to transfer data should be limited according to the sensitivity of the data being transferred. Staff must always check that information is being sent to the appropriate recipient. It is strongly suggested that to send sensitive personal data staff use recorded delivery mail which can be tracked or delivered by hand if encryption facilities are not available.

- 3.28 Staff should not share or give out passwords and should not permit anyone without clearance to access secure information.
- 3.29 The Computer Misuse Act makes it an offence to access any computer system for which access authorisation has not been given. Any attempt to interfere with or try to bypass the security controls on a computing system is an offence. Similarly trying to obtain information, such as 'users' passwords or accessing or modifying files belonging to other people who have not given access authorisation is also an offence.

Cloud Computing

- 3.30 Only cloud computing networks or services, including social media commissioned by the Academy, or expressly authorised by the Data Protection Officer, may be used to store and send information concerning or relating to Academy business. The use of personal cloud storage solutions (OneDrive Personal, iCloud, G-Drive etc.) for the transfer of Academy information is expressly forbidden.
- 3.31 Personal Data, Special Category Personal, confidential and sensitive information, whether on the Academy network or a Client Device must not be stored on a cloud computing network or service not commissioned by the Academy, or expressly authorised by the Data Protection Officer.
- 3.32 If Data or other information concerning or relating to Academy business is to be stored in or on a cloud network, the Academy will take all reasonable steps to find out in which country the Data or other information is being stored, and to ensure that appropriate measures are in place in relation to any Data transferred outside of the EEA.
- 3.33 If the Academy receives notification that Data in respect of Academy business has been corrupted, lost or otherwise compromised while stored on a cloud network, the Academy should ascertain whether any or all of the information stored in the cloud can be recovered and if this is possible restore that information.
- 3.34 Any corruption, loss or compromise of information held on a cloud network should be reported to the Network Manager.

Secure Disposal

- 3.35 All confidential waste paper should be shredded and / or disposed of through a confidential waste service. This includes personal data due for destruction, duplicates of personal data and other confidential information.

- 3.36 Computer systems must be fully cleansed of any information before they are disposed of or re-sold. Approval and support for this must be obtained from the ICT Network Manager. Discs and other removable devices should be destroyed if they are intended for disposal.

Security of buildings

- 3.37 All staff will be issued with ID badges. Staff should be prepared to challenge any person in the academy without an academy issued visitor badge to ensure that they have a right to be there.
- 3.38 Any contractor should carry identification and show this on request. All contractors will need to sign in and sign out at the academy office and wear an academy issued visitor badge.
- 3.39 Staff should ensure that windows and external doors are locked when a classroom or office is empty, and at the end of school, and that offices, filing cabinets and cupboards are also kept locked if required. The only exception is in the event of a fire evacuation when all doors other than the Finance and Exams offices must be left unlocked.
- 3.40 Any security concerns including break-ins and loss of computer equipment must be reported to the Headteacher who will decide on the appropriate course of action which may include notifying the Police.

Email security

- 3.41 Staff must bear in mind that email is a formal record of correspondence and can be subject to requests under GDPR (Subject Access Requests) and Freedom of Information legislation – emails may be retained as records on staff, pupil and school files.
- 3.42 Staff must not send anything which would be unlawful or discriminatory, or whose content is defamatory or libellous. Work emails should not be used for forwarding chain letters or similar 'spam'. The Telecommunications Act 1994 makes it an offence to transmit messages or other matter via a public telecommunications system that is indecent, obscene or menacing. This includes causing annoyance, inconvenience or needless anxiety to another by a message that the sender knows to be false.
- 3.43 If members of staff receive an email which breaches IMAT policies or breaks the law, they are advised to speak to a senior staff member of staff or the Network Manager before responding. This includes 'spam' emails, particularly those purporting to be from banks, or any email asking the recipient for money.

INSIGHT MAT POLICIES AND PROCEDURES

- 3.44 Staff should re-read any message before sending, checking for clarity and content (including grammar), and ensure that the message is being sent to the appropriate recipient.
- 3.45 Do not use email if the information being sent is personal or confidential, unless you are certain the information will be secure for example through password protection or encryption.
- 3.46 Do not use email to anyone who is known not to check emails regularly, or where a phone call or meeting would be a more appropriate way to get the message across.
- 3.47 Do not use email where there may be a contractual or legal need to provide a written and signed document or prove the identity of the sender.
- 3.48 Do not click on links from external emails unless you are sure of the sender. Staff should be aware of phishing emails.

Internet security

- 3.49 Access to the Internet must be used responsibly and legally. Staff must not take *any* action which could bring the Trust into disrepute, cause offence, interfere with the organisation's work or jeopardize the security of data, networks, equipment or software.
- 3.50 With the advent of e-commerce, staff should beware of committing the academy to purchase or acquire goods or services without proper authorisation. Purchase Requisitions must be raised for all goods and services.
- 3.51 Staff must not attempt to download or install unauthorised software from the internet. All software should be approved by the ICT Network Manager.
- 3.52 Staff should be aware that, as with paper sources, not all information on the internet is accurate, complete or reliable. Users should ensure its validity, as they would printed publications, before using it.
- 3.53 At any time and without prior notice, the IMAT reserves the right to examine e-mail, personal file directories, and other information stored on the Trust and Schools' network, equipment or cloud storage. Permission to examine such information will only be granted by the Chief Executive Officer.

Security of records

- 3.54 Access to data, and particularly personal data, should be limited to staff who have a genuine need to know.

- 3.55 Changes to data, and particularly personal data, should be carried out promptly.
- 3.56 Records should be properly managed to enable staff to find or identify information quickly and accurately.

Reporting & responding to security breaches

- 3.57 Any security breaches or loss of personal data must be immediately reported to the Headteacher who in turn will inform the CFO and the Data Protection Officer (DPO). The form at **Appendix 2** must be completed.
- 3.58 A security breach would be caused when [and this not an exhaustive list]:
- A laptop containing personal data is lost or stolen
 - A USB [memory stick] containing personal data is lost or stolen
 - A vehicle containing a laptop or paper files is stolen
 - A laptop or paper files are stolen from a private property
 - An email is sent [either internally or externally] with files attached containing personal data and the email is sent to the wrong email address
 - An email is sent [either internally or externally] with files attached that contain personal data which is far in excess of that necessary for the business function to be carried out
 - An email is sent [either internally or externally] which should be sent "bcc" to a large number of people, is instead, sent "to" and so the recipient is aware who else has received the email and their personal email address or other personal details
 - Personal data is shared outside of the academy for a legitimate business reason, but it is lost by the recipient, or it is stolen from the recipient, or it is used by the recipient in a manner for which they have no authority for
 - Personal data is transferred electronically outside the academy and is not encrypted or password protected when it should be
 - Paper files of personal data are left unattended and are taken or copied and then used for an unauthorised purpose
 - A member of staff uses personal data for a personal rather than an academy or Trust business reason
- 3.59 Any theft from the academy should be notified to the Headteacher who will decide on the appropriate course of action which may include notifying the Police.
- 3.60 Any loss of or damage to technical equipment should be notified to the ICT Network Manager.
- 3.61 The CFO and the DPO, with support from the Headteacher and where necessary the Network Manager for cases involving breaches of IT security, will investigate the

security breach / loss of data through the process detailed at **Appendix 2**. The investigation will determine whether to notify the Information Commissioner (ICO).

4. Monitoring and Evaluation

The IMAT Board will formally review this policy according to the policy schedule or more frequently if circumstances or legislation suggest it is appropriate.

Appendix 1

INFORMATION ASSET AUDIT FORM

1. What is an information asset audit?

An information asset audit is a form of records survey encompassing:

- Paper documents and records
- Electronic documents and records
- Databases (proprietary or developed in-house)
- Microfilm/microfiche
- Sound recordings
- Video/photographic records (including those records taken on traditional magnetic tape and photographic paper but increasingly digital sound, video and photo files)
- Hybrid files
- Knowledge

The information audit is designed to help organisations complete an information asset register and to identify vital information. The terminology grows out of the concept of “knowledge management” which involves the capture of knowledge in whatever form it is held, including encouraging people to document the information they would previously have held in their heads. It is now generally accepted that information is an organisation’s greatest asset and that it should be managed in the same way as the organisation’s more tangible assets such as staff, buildings and money.

Effective Information Management is about getting the right information to the right people at the right time and an information audit is key to achieving this.

2. What are the benefits of the information asset audit?

The information audit is designed to allow organisations to discover the information they are creating, holding, receiving and using and therefore to manage that information in order to get the most effective business use from it. For an academy the concept is much more concerned with accessibility of information. The information audit allows the academy to identify the personal information it creates and stores to allow correct management under the Data Protection Act (DPA) 1998.

INSIGHT MAT POLICIES AND PROCEDURES

INFORMATION ASSET AUDIT FORM

Name of Academy	
Room within Academy / Office (if appropriate)	
Person responsible for keeping the information (name & job title)	
Where the information came from / originated (if different from above)	
Detailed description of the information	
How is the information stored?	
Purpose for keeping the information (e.g. staff admin, student admin, marketing, financial, statistical, research, etc etc.)	
Format e.g. paper, electronic, database, spreadsheet, disk, CD, video, photo (could be more than one)	Paper Electronic Film
If electronic which format?	Floppy Disk Databases (proprietary or developed in house) Microfilm/Microfiche Sound Recordings Video/Photographic Records Hybrid Files Server Hard Drive CD Tape Other: Please Specify
Location of information	
How often is the information accessed	Less than once a month At least once a week but not every week At least once a week but not every day Daily
How long do you need to keep this	Less than 1 year Less than 2 years

INSIGHT MAT POLICIES AND PROCEDURES

information- refer to Information & Record Management Society Retention Guidelines: Records Management Toolkit	2 to 6 years 6 to 10 years 10 to 25 years 25 to 50 years 50 to 100 years Archived for research
Is the information disposed of at the end of its use? If so, how?	
<i>If the information you hold is personal data, i.e. it is about, or contains information about, an individual (could be staff, student or an external person), please answer the following questions. If you have a form which is used to collect personal data, please provide a copy of that form.</i>	
Who is the information about? E.g. staff, student, other: please give as much information as possible.	
What information is held? E.g. contact details, marks or progression, meetings about the person, biographical data, sickness, salary, etc. etc. Does any of this information fall under special category data (GDPR)? (Please specify) i.e. <ul style="list-style-type: none"> • Racial or ethnicity • Political opinions • Religious/Philosophical beliefs • TU Membership • Health • Sex life/Sexual Orientation • Genetic/Biometric Information 	
Does the person whose information you hold know that it is held? Have they been informed? Have they signed a consent form? (Please provide as full detail as possible.)	
Is the information subject to automatic decision-making? (i.e. without human intervention)	

INSIGHT MAT POLICIES AND PROCEDURES

Is the information disclosed outside the Trust? If so, to whom? (If it is abroad, please state which country.)	
Do you have any method for checking the accuracy of the information held, at regular intervals? Please give details.	
Please provide the following detail about the information that you hold, whether it is personal data or not.	
What security arrangements, if any, do you have for the location of the information? (Both hard & soft copy.)	
Is the information made available on your website, and if so, is it Intranet only or available to all?	
If not available, is there any reason why it should not be?	
The loss of certain information through fire or some other disaster would have very serious consequences for the academys operations	Does this information fall into this category? Yes No If yes explain why:
Any other comments	

Name:

Contact details:

Date:

Please return this form to the Responsible Officer, Insight Academy (insert name)

INSIGHT MAT POLICIES AND PROCEDURES

Audit Recommendations for this item (insert as appropriate)	Actions	By who	By when	Verified by:
Move to secure unit				
Record destruction				
Archive				
Restrict Access to?				

DATA BREACH / INCIDENT FORM

Please complete this form if you have detected or been advised of a data security incident or breach. It is imperative that you complete this form immediately upon detection and where possible, please advise your Headteacher (or any member of the Leadership Group) of the suspected breach immediately.

Once completed, please email this form to DPO@sirgrahambalfour.staffs.sch.uk and send a copy to the Headteacher and Academy day to day DPO manager:

Incident / breach details	
Name and contact details of person reporting incident:	
Nature of the incident/ breach: (e.g. theft, disclosed in error, technical problem, inaccurate information on system...)	
Date(s) incident took place:	
Date you detected the incident:	
Brief description of how you became aware of the incident:	
Brief description of the incident including details of the data, records or systems believed/ potentially affected:	
Approximate number of affected data subjects, if known:	
Have the affected individuals been informed of the incident:	
Is there any evidence that the personal data involved in this incident has been further disclosed: Please provide details:	

INSIGHT MAT POLICIES AND PROCEDURES

What measures have been taken to minimise the impact of the incident and avoid future reoccurrences:	
Has the data been retrieved or deleted? If yes, state when and how:	

INVESTIGATION

Assessing the risks and actions to be taken

The Academy day to day Data Protection Officer will liaise with the Headteacher and where necessary the Network Manager and information asset owners to consider the following risk factors when assessing, managing and investigating the incident. This list is not intended to be prescriptive and other relevant factors and issues should be recorded as necessary

Incident summary

Summary of the actual or suspected security breach

--

Date of incident:

Academy(s) / services affected:

People involved in/affected by the incident, (such as staff members, students, contractors, external clients)

INSIGHT MAT POLICIES AND PROCEDURES

Does the incident need to be reported immediately to the police? YES/NO

Risk Factor Details and action required

Which IT systems, equipment or devices are involved in the security breach?	
What information has been lost or compromised?	
How much information has been lost?	
Is the information unique?	
If the incident involves the loss of a laptop or portable device how recently was the information it held backed up onto central IT systems?	
How important is the information or system to the Academy/Trust? Is it business-critical? Do users rely on access to this particular information asset or can they use reliable electronic copies or alternative manual processes e.g. paper files if the information asset is unavailable?	
How urgently would access need to be restored to an information asset to resume business or, if a workaround will keep business moving in the short term, to return to the required standard of service?	
Will the loss or compromise of the information have adverse operational, research, financial legal, liability or reputational consequences for the Academy/Trust or third parties?	

INSIGHT MAT POLICIES AND PROCEDURES

Is the information bound by any contractual security arrangements?	
<p>Is any of the information confidential? Please provide details of any types of information that fall into any of the following categories.</p> <p>Personal data eg name, address, age Special Category Data (as defined in GDPR) relating to an identifiable individual's</p> <ol style="list-style-type: none"> 1. race or ethnicity; 2. political opinions; 3. religious /Philosophical beliefs; 4. TU membership; 5. health; 6. sex life/Sexual Orientation; 7. Genetic/Biometric Information 	
Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as national insurance numbers and copies of passports and visas.	
Personal information relating to vulnerable adults and children.	
Detailed profiles of individuals; including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed.	
Spread sheets of marks or grades obtained by students, information about individual cases of student discipline.	
Sensitive negotiations which could adversely affect individuals.	

INSIGHT MAT POLICIES AND PROCEDURES

Security information that would compromise the safety of individuals if disclosed.	
Any other personal information that would cause damage or distress to individuals if disclosed without their consent. Other categories of "high risk" Information.	
Information received in confidence .e.g. legal advice from solicitors, trade secrets and other proprietary information received from contractors, suppliers and partners Information that would substantially prejudice the Trust or another party's intellectual property rights, commercial interests or competitive edge if it were disclosed.	
Information that would compromise the security of buildings, equipment or assets if disclosed.	
Who else needs to be informed	
Reported to Police?	YES/NO If YES notified on: Incident ref:
Major risks escalated to Audit Committee and Risk Management Register	YES/NO If YES: Date
Notification to Information Commissioner's Office (within 72 hours)	YES/NO If YES notified on [date]
Notification to data subjects	YES/NO If YES notified on [date]

INSIGHT MAT POLICIES AND PROCEDURES

Notification to other external, regulator/stakeholders	YES/NO If YES notified on
-----------------------------------------------------------	----------------------------------

INSIGHT MAT POLICIES AND PROCEDURES

Reviewing the incident

The DPO and Responsible Officers should meet to review the incident, ensure that all appropriate actions have been taken to mitigate its impact of the incident and to identify further action needed to reduce the risk of a future breach of this kind.

How and why the incident occurred:
Actions taken to resolve the incident and manage its impact:
Impact of the incident: (Operational, financial, legal, liability, reputational)
Risks of other adverse consequences of the incident: (Operational, financial, legal, liability, reputational)
Any further remedial actions required to mitigate the impact of the breach:

INSIGHT MAT POLICIES AND PROCEDURES

Actions recommended to prevent a repetition of the security breach:

Resource implications or adverse impacts, if any, of these actions:

INSIGHT MAT POLICIES AND PROCEDURES

APPENDIX 3

INSIGHT MULTI-ACADEMY TRUST - EQUIPMENT LOAN LOG

FOR ALL LAPTOPS, PROJECTORS, CAMERAS ETC.

Please record all items going out on loan and sign back in, as and when returned.

Date	Time	Item	Serial Number	Taken By (Name)	Planned return Date	Return Date	Return Time	Returned To (Technician Name)

The person who borrows the equipment is responsible for its safe return in the condition in which it was loaned. Loss or damage must be reported to the Head of Faculty upon return to the Department.

INSIGHT MAT POLICIES AND PROCEDURES

APPENDIX 4 TEACHER LAPTOP FORM

Date	Laptop Serial Number	Taken By (Name)	State of laptop on handover	Return Date	State of laptop on return	Returned To (Technician Name)