



**ONLINE  
POLICY**

## INSIGHT MAT POLICIES AND PROCEDURES

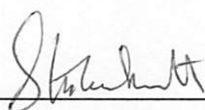
### CHANGE CONTROL

<b>Date</b>	<b>Issue</b>	<b>Details of change</b>
07/04/2017	0.a	Initial Draft
30/06/2017	0.b	Updated following review by Trustees
19/07/2017	1.0	Updated following approval at Board Meeting 18/07/2017
27/11/2019	1.0	Policy name change – No further changes
21/06/2021	1.a	Updated following review
30/06/2021	2.0	Policy updated following Board Approval at meeting on 30/06/2021
Summer 2023	2.a	Updated following review
Summer 2023	3.0	Policy updated following Board Approval at meeting on 14.06.2023

### AUTHORISATION

Approved at Board Meeting on 14<sup>th</sup> June 2023

Signed:



14-6-23

**Chair of Trust Board**

**Date**

# **INSIGHT MAT POLICIES AND PROCEDURES**

## **Online Policy and Procedure**

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

### **Introduction**

ICT in the 21<sup>st</sup> Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, academies need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Office 365 (Microsoft Teams, Sharepoint etc.)
- E-mail
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Social Media

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

Within IMAT we understand the responsibility to educate our students on online issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Policy (for all staff, governors, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the academy (such as PCs, laptops, webcams, whiteboards, voting systems, digital video equipment, tablets etc); and technologies owned by staff, but brought onto academy premises (such as laptops, mobile phones, camera phones, etc).

## **INSIGHT MAT POLICIES AND PROCEDURES**

### **Aim**

IMAT believes that online safety (online) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, mobile phones or games consoles.

IMAT accepts that the internet and information communication technologies are an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

IMAT has a duty to provide the academy community with quality Internet access to raise education standards, promote student achievement, support professional work of staff and enhance the academy's management functions. The IMAT also identifies that with this there is a clear duty to ensure that children are protected from potential harm online.

The purpose of this Online Policy is to:

- Clearly identify the key principles expected of all members of the community with regards to the safe and responsible use technology to ensure that the IMAT is a safe and secure environment.
- Safeguard and protect all members of the MAT's community online.
- Raise awareness with all members of the MAT's community regarding the potential risks as well as benefits of technology.
- Enable all staff to work safely and responsibly, to role model positive behaviour online and be aware of the need to manage their own standards and practice when using technology.
- Identify clear procedures to use when responding to online safety concerns that are known by all members of the community.

This policy applies to all Members, Trustees, Local Governing Body members, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the IMAT (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

This policy applies to all access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with academy issued devices for use off-site, such as a work laptop or mobile phone. This policy must be read in conjunction with other relevant academy policies including (but not limited to) Safeguarding, Anti-bullying, Behaviour, Acceptable Use Policies, Confidentiality.

### **Key Elements**

#### **Roles and Responsibilities**

## **INSIGHT MAT POLICIES AND PROCEDURES**

As online is an important aspect of strategic leadership within the IMAT, the Trustees and Local Governing Bodies have ultimate responsibility to ensure that the policy and practices are embedded and monitored. There is a named Designated Safeguarding Lead in each establishment who has been designated this role as a member of the senior leadership team. All members of the academy community have been made aware of who holds this post. It is the role of the Designated Safeguarding Lead to keep abreast of current issues and guidance through organisations such as Entrust, CEOP (Child Exploitation and Online Protection) and Childnet.

Senior Management, Governors, Trustees and Members are updated by the relevant Designated Safeguarding Lead and all have an understanding of the issues and strategies within IMAT in relation to local and national guidelines and advice.

This policy, supported by the IMAT's Acceptable Use Agreement for staff, governors, visitors and students, is to protect the interests and safety of the whole MAT community. It is linked to the following mandatory MAT policies: Safeguarding, Health and Safety, Home-academy agreements, Behaviour Policy, Anti-Bullying Policy.

### **Online skills development for staff**

- Our staff receive information and training on online issues in the form of updates via Academy Bulletins, website and INSET.
- New staff will receive information on an academy's acceptable use policy as part of their induction.
- All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of online and know what to do in the event of misuse of technology by any member of the academy community.
- All staff are encouraged to incorporate online activities and awareness within their curriculum areas.

### **Online in the Curriculum**

ICT and online resources are increasingly used across the curriculum. We believe it is essential for online guidance to be given to the students on a regular and meaningful basis. Online is embedded within our curriculum and we continually look for new opportunities to promote it.

- IMAT provides opportunities within a range of curriculum areas to teach about online safety.
- Educating students on the dangers of technologies that maybe encountered outside school is done informally when opportunities.
- Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

## **INSIGHT MAT POLICIES AND PROCEDURES**

- Students are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Students are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline/ CEOP report abuse button.
- Students are taught to evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum

### **Password Security**

Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

- All users read and sign an **Acceptable Use Policy** to demonstrate that they have understood IMAT's Online Policy.
- Users are provided with an individual network login the same which is used for Office 365 which includes e-mail, Teams and Sharepoint. From Year 7 they are also expected to use a personal password and keep it private.
- Staff have a two-factor authentication system.
- All users have to change their passwords every 12 months.
- Where an academy has subscribed to SIMS student, this is used in order to access information about timetables, merits, demerits etc.
- Students are not allowed to deliberately access on-line materials or files on the academy system of their peers, teachers or others.
- If a user thinks their password may have been compromised or someone else has become aware of their password, report this to the Network Manager.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of academy systems and SIMs systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. Due consideration should be given when logging into the academy systems where information is cached on personal devices.
- In our MAT, all ICT password policies are the responsibility of the Network Manager and all staff and students are expected to comply with the policies at all times.

## **INSIGHT MAT POLICIES AND PROCEDURES**

### **Data Security**

The accessing and appropriate use of academy data is something that the academy takes very seriously.

- Staff are aware of their responsibility when accessing academy data. Level of access is determined by the Trust Board.
- Any confidential data taken off the academy premises must be encrypted.
- Data can only be accessed and used on academy computers or laptops. Staff are aware they must not use their personal devices for accessing any ***academy/ children/student*** data.

### **Managing the Internet**

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The academy ensures students will have supervised access to Internet resources (where reasonable) through the academy's fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with students.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents/carers recheck these sites and supervise this work. Parents/Carers will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute academy software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

### **Infrastructure**

- The current members of IMAT have a monitoring solution called SENSO Safeguarding where academy device activities are monitored and recorded.
- SENSO Safeguarding software and RM SafetyNet are monitored by the ICT Technicians.
- IMAT is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

## **INSIGHT MAT POLICIES AND PROCEDURES**

- Staff and students are aware that academy based e-mail and internet activity can be monitored and explored further if required.
- IMAT does not allow students access to internet logs.
- IMAT uses management control tools for controlling and monitoring workstations.
- If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the Designated Safeguarding Lead.
- It is the responsibility of the individual academy, by delegation to the Network Manager, to ensure that Anti-virus protection is installed and kept up-to-date on all academy machines.
- Students using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not IMAT's responsibility nor the Network Manager's to install or maintain virus protection on personal systems
- Students and staff are not permitted to download programs or files on academy-based technologies without seeking prior permission from the ICT technicians.
- If there are any issues related to viruses or anti-virus software, the Network Manager should be informed via an e-mail.

### **Managing other Web technologies**

- At present, IMAT endeavours to deny access to social networking sites to students and staff within the academy.
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, academy details, IM/ e-mail address, specific hobbies/ interests).
- Our students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our students are asked to report any incidents of bullying to the academy.
- Staff may only create blogs etc. in order to communicate with students using the Learning Platform/VLE/Gateway or other systems approved by the IMAT.



## **INSIGHT MAT POLICIES AND PROCEDURES**

### **Mobile technologies**

Technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Technologies will be examined for educational benefit and the risk assessed before use in school is allowed. IMAT chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

### **Personal Mobile devices (including phones)**

- IMAT allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the IMAT allow a member of staff to contact a student or parent/ carer using their personal device whilst on academy premises.
- Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within the academy buildings. At all times the device must be switched onto silent and kept in their bags.
- This technology may be used, however for educational purposes, as mutually agreed with the relevant Headteacher. The device user, in this instance, must always ask the prior permission of the bill payer.
- The academy is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the academy community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

### **Academy provided Mobile devices (including phones)**

- The sending of inappropriate text messages between any member of the IMAT community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the IMAT community.
- Where the academy within IMAT provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.
- Where the academy within IMAT provides a laptop for staff, only this device may be used to conduct academy business outside of the building.

## **INSIGHT MAT POLICIES AND PROCEDURES**

### **Managing e-mail**

The use of e-mail within most academies is an essential means of communication for both staff and students. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between academies on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an e-mail in relation to their age and demonstrate good etiquette.

- IMAT gives all staff and students their own e-mail account to use for all academy business. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. This should be the account that is used for all academy business.
- Under no circumstances should staff contact students, parents or conduct any academy business using personal e-mail addresses.
- The academy includes a standard disclaimer that is attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the academy or IMAT'.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on academy headed paper.
- Students may only use academy approved accounts on the academy system.
- The forwarding of chain letters is not permitted. Students and staff must alert the Network Manager if they receive mail that causes offence or anxiety.
- 'Spamming' is not allowed under any circumstances.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Students are not allowed to 'chat' via the academy's e-mail system
- Staff must inform (the relevant Designated Safeguarding Lead/ line manager) if they receive an offensive e-mail.
- Students are introduced to e-mail as part of their Computing lessons.

### **Safe Use of Images**

#### **Taking of Images and Film**

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any

## **INSIGHT MAT POLICIES AND PROCEDURES**

member of the academy community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of students) and staff, IMAT permits the appropriate taking of images by staff and students with academy equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the academy's network and deleted from the staff device.
- Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the academy's network and deleted from the student's device.

### **Consent of adults who work at the academy**

- Permission to use images of all staff who work within the IMAT is sought on induction and a copy is located in the personnel file

### **Publishing students' images and work**

On a child's entry to the academy, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the academy web site
- In the academy prospectus and other printed publications that the academy may produce for promotional purposes
- Recorded/ transmitted on a video or webcam
- In display material that may be used in the academy's communal areas
- IN display material that may be used in external areas, i.e. exhibition promoting the academy
- General media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this academy unless there is a change in the child's circumstances where consent could be an issue, e.g divorce of parents, custody issues, etc.

Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid.

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.

## **INSIGHT MAT POLICIES AND PROCEDURES**

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Only the Web Manager has authority to upload to the site.

### **Storage of Images**

- Images/ films of children are stored on the academy's network/Cloud Storage and staff laptops
- Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of their Headteacher
- Rights of access to this material are restricted to the teaching staff and students within the confines of the academy network/Cloud storage.
- Admin staff have the responsibility of deleting the images when they are no longer required, or the student has left the academy.
- Teachers must not store images of academy events for prolonged periods of time on their laptops.

### **Webcams and CCTV**

- Academies may use CCTV for security and safety. The only people with access to this are the site management team and the academy's Leadership Team. Notification of CCTV use is displayed at the front of each academy.
- We do not use publicly accessible webcams in the academy building.
- Webcams in the academy building are only ever used for a specific learning purpose.

Misuse of the webcam by any member of the academy community will result in sanctions (as listed under the 'inappropriate materials' section of this document). Consent is sought from parents/carers and staff on joining the academy, in the same way as for all images.

### **Misuse and Infringements**

#### **Complaints**

Complaints relating to Internet Safety should be made to the Designated Safeguarding Lead or Headteacher. Incidents should be logged and IMAT **Flowcharts for Managing an Online Incident** should be followed.

#### **Inappropriate material**

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Designated Safeguarding Lead.

## **INSIGHT MAT POLICIES AND PROCEDURES**

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Designated Safeguarding Lead, depending on the seriousness of the offence; investigation by the Headteacher, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Students are made aware of sanctions relating to the misuse or misconduct via ICT lessons

### **Equal Opportunities**

#### **Students with additional needs**

The academy endeavours to create a consistent message with parents/carers for all students and this in turn should aid establishment and future development of the academy's Online rules.

However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of online safety. Internet activities are planned and well managed for these children and young people.

#### **Parental Involvement**

We believe that it is essential for parents/carers to be fully involved with promoting online safety both in and outside of school. We regularly consult and discuss online safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the academy.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on academy website)
- The academy disseminates information to parents relating to online safety where appropriate in the form of;
  - Information and celebration evenings
  - Posters
  - Website
  - Newsletter items

## **INSIGHT MAT POLICIES AND PROCEDURES**

### **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.