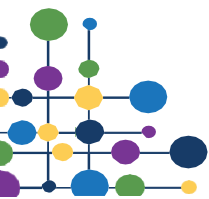


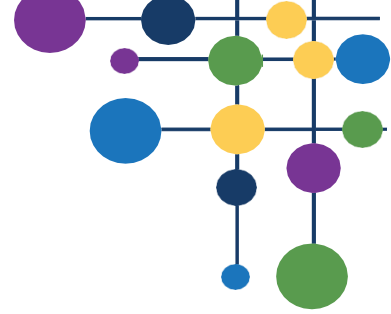


ICT POLICY & PROCEDURE

MAT Version	2.5
Name of Policy Writer	Natalie McSheffrey
Last reviewed	April 2023
Date of next review	April 2025
Approved by Directors	21 st March 2024

Schedule of amendments:
v2.5 – updates to section 8, 10 and 17





SHARE MAT Policy for ICT

CONTENTS

Section 1 Introduction

Section 2 Purpose and Scope

Section 3 ICT Security

Section 4 ICT Administration Team

Section 5 Software and Licensing

Section 6 Security and Inventories

Section 7 Insurance

Section 8 Fault Reporting and General use

Section 9 Authorisation and Access

Section 10 Staff Devices

Section 11 Remote/Home Working

Section 12 E-mail System

Section 13 Use of the Internet and E-mail

Section 14 Monitoring use of the Internet

Section 15 File Downloading

Section 16 Chats and Newsgroups

Section 17 Passwords

Section 18 Security

Section 19 Backing Up and Disaster Recovery

Section 20 Photographs and Photography

Section 21 Use of Digital Cameras

Section 22 Social Media

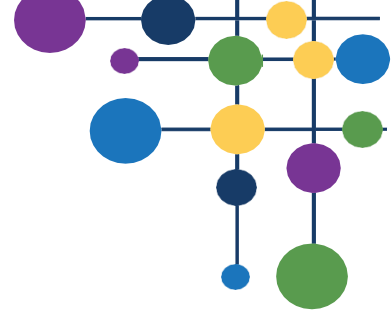
Section 23 Personal Use of Social Media

Section 24 Mobile Phones and Personal Devices

Section 25 Public Wi-fi Acceptable Use

Section 26 Breaches





Section 1 Introduction

SHARE MAT is committed to developing the use of ICT throughout the organisation and to developing the skills and knowledge of parents, staff, students and the wider community.

ICT is used by students to assist their work and learning, by teaching staff as a support to their teaching and administrative work and by support staff to provide effective and efficient support for school systems and procedures.

ICT and computing encompasses every part of modern life and it is important that our students are taught how to use these tools and more importantly how to use them safely. It is important for students, staff and the wider community to have the confidence and ability to use these tools to prepare them for an ever changing and rapidly developing world. To enable our students and staff to be confident, competent users and learners of ICT and computing we aim to:

- Use computing and ICT where appropriate to ensure students are motivated and inspired in all areas of the curriculum.
- Use computing and ICT to help improve standards in all subjects across the curriculum.
- Develop the competence and skills of students through Computing lessons and provide them with the chance to consolidate these in a cross curricular context.
- Ensure students are challenged in their use of Computing and are provided with exciting, creative ways in which to share their learning.
- Use tools available to ensure children have the ability to work independently and collaboratively to suit the needs of the situation.
- Provide all staff and students with training and support to ensure that they can, and have the confidence to, use computing to its full potential in all aspects of school life, safely and securely.
- Use computing and technology as a form of communication with parents, students and the wider community.

Section 2 Purpose and Scope

- This policy applies to the whole MAT community including the Directors, Governing Bodies, Senior Leadership Teams, all staff employed directly or indirectly by the MAT, all students and visitors.
- The Directors will ensure that any relevant or new legislation that may impact upon the provision for online safety within the MAT will be reflected within this policy.

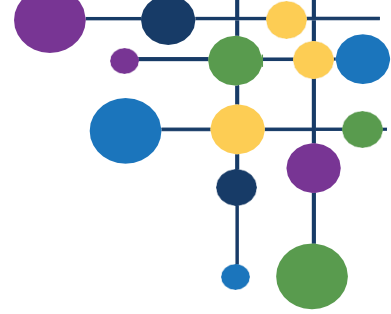
Section 3 ICT Security

Whilst considering its responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, the trust does all that it reasonably can to limit children's exposure to the risks from the trust's IT system.

SHARE MAT's internet access is governed by a web filtering system which specialises in web security and filtering for the Internet in large organisations and schools, which has been DfE approved.

The web filtering system delivers highly accurate real-time filtering results - it examines the content, context and construction of every web page requested. All undesirable material (including anonymous proxies & online games) can be detected and blocked without disrupting learning-based web resources. Social media, file sharing and other potential distractions can be blocked completely or managed effectively.





By adhering to the highest filtering and security standards, the system protects students, staff and the trust from the increasing threat of litigation from inappropriate or illegal on-line activities. It allows our schools to focus on education without worrying about web security issues.

The system will block any websites it sees as a threat. If staff need access to a specific website for educational purposes, then please see the IT Manager, who will have the final say as to whether the site is deemed appropriate. It is an offence to try and bypass the system yourself to gain access to websites.

Please be aware that the system monitors and logs every webpage and Internet request from all school curriculum users (staff and students.)

Whilst the system is a very powerful web filter, users need to be aware that on occasions, a website is not identified correctly for a number of reasons. If any user gains access to a website inappropriate for a school audience, this must be reported to IT Support immediately for inclusion on the block list.

The IT team will immediately report any inappropriate, suspicious or illegal online activity by students to the Designated Safeguarding Lead.

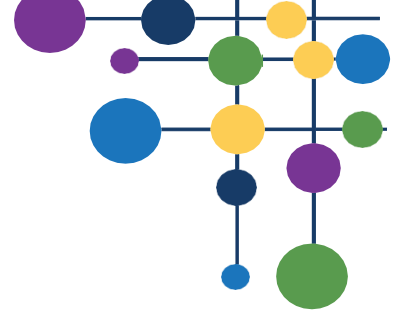
The IT team will immediately report any inappropriate, suspicious or illegal online activity by staff to the Headteacher.

Cyber Security

The Trust has adopted the NCSC 10 step guidance that aims to help organisations manage their cyber security risks. Adopting these security measures covered by the 10 Steps reduces the likelihood of cyber-attacks occurring and minimises the impact when incidents do occur. The 10 steps are:

1. **Risk management** – Identify data and systems that are potential risk targets.
2. **Identity and access management** - Control who and what can access your systems and data
3. **Engagement and training** - Collaboratively build security that works for people in our organisation. Produce user security policies covering acceptable and secure use of our systems. Maintain awareness and staff training of cyber risk.
4. **Data security** - Protect data where it is vulnerable. Produce relevant policies and establish anti-malware defences across your organisation which include data backups.
5. **Asset management** – Maintain an asset register for data and systems throughout the Trust.
6. **Logging and monitoring** - Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.
7. **Architecture and configuration** - Design, build, maintain and manage systems securely. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls. 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.
8. **Incident management** - Plan our response to cyber incidents in advance using a maintained disaster recovery plan.
9. **Vulnerability management** - Keep our systems protected throughout their lifecycle using relevant antivirus software, firewalls and limiting access controls.



- 
10. **Supply chain security** - Collaborate with your suppliers and partners that they are compliant with legal requirements and that data given to third parties is safe and secure.

Section 4 ICT Administration Team

ICT will be used wherever possible to assist staff in their roles and responsibilities, to provide data as appropriate and to assist in the management of school systems, e.g. finance, attendance, performance monitoring.

Any faults discovered with ICT equipment or software should be reported to IT Support. Under no circumstances should staff or students attempt to repair or disassemble any MAT owned equipment.

Staff are permitted to connect their own personal device(s) to the staff Wi-Fi network.

Students are not permitted to connect personal devices to the Trust Wi-Fi, an exception to this is the sixth form college. A segregated network is provided that is secure and closely monitored with limited access to the internet.

Section 5 Software and Licensing

Software used on ICT resources must solely be that which has been purchased with an accompanying individual or site licence. This means that the software is licensed for use (either unlimited or limited to a number of machines at any one time) on the school site only.

Additional licences may be purchased by the MAT where colleagues are required to undertake work at home on specific software. The IT Manager will monitor and authorise all requests for such software.

Any software purchases and/or online subscriptions should firstly be discussed with the IT Manager and when the software arrives in the MAT it is registered centrally with the IT Team for secure storage and installation.

Software audits will be carried out on a regular basis to ensure no unlicensed software is being used in the MAT. Records are kept detailing what software is installed on which machines in order to ensure that the MAT is fully compliant with its entire software license.

Staff members who are concerned that unlicensed software might be being used should discuss the matter with the IT Manager.

Under no circumstances must copies of any software be transferred to or from any off site system unless the appropriate licence has been purchased and software cannot be hired or sold on to another user. Installation of software is the sole responsibility of the IT Manager.

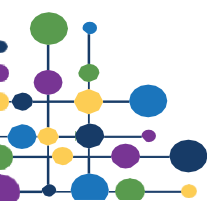
CDs etc. of purchased software must be given to the IT Manager on receipt and original copies of licences etc. will also be kept by the IT Manager.

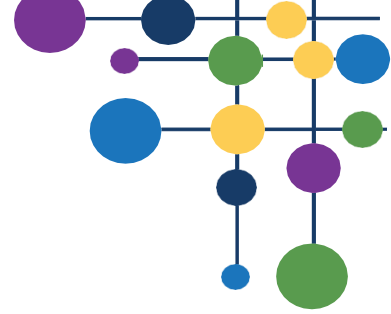
The IT Manager will maintain an inventory of software installed and will determine whether additional licences need to be purchased.

Section 6 Security and Inventories

Items will be added onto the MAT's ICT inventory maintained by the IT Manager. Where possible, serial numbers should be recorded for all items.

The MAT's ICT inventory will provide an overview of all resources within the MAT and provide a profile of each machine.





Section 7 Insurance

Staff wishing to continue curriculum development or professional development by making use of MAT owned systems outside school hours and off the premises should first discuss the matter with the IT Manager.

The MAT has insurance to cover the theft of hardware and software from the premises only.

All staff and students are encouraged to adopt practices which will encourage the good security of rooms and equipment.

Section 8 Fault Reporting and General Use

Staff are required to report all issues, faults and damage to ICT equipment by using the below escalation procedure:

1. Every system – Staff are required to raise a ticket for all IT issues on Every for compliance and report monitoring purposes.
2. IT support email – must only be used for more urgent IT assistance, an Every ticket must still be raised.
3. Phone – Only in emergency, an Every ticket must still be raised.

General use

Effective virus protection software is installed on the MAT network. If, however, staff discover anything strange about the PCs after memory sticks, CDs, DVDs brought into the MAT have been used, they should report it to IT Support.

All IT equipment is recorded in an asset register detailing its type and location. Staff are not permitted to move any devices without first notifying the IT Team.

All staff members have a responsibility to ensure ICT resources and equipment are checked after use and are left in good working order for others to use. Staff members detecting any damage or malfunction should report it to the IT Team.

All staff members must ensure that equipment, including projectors, is turned off after use to prolong equipment life and energy efficiency.

All ICT users, staff and students have a responsibility to the whole ICT user community.

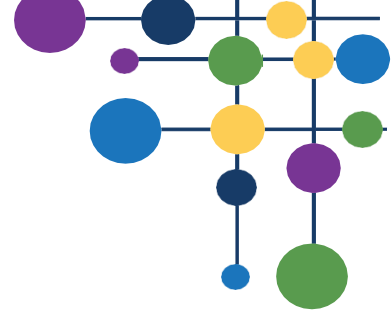
Section 9 Authorisation and Access

Levels of access will be established for different users on the networks and systems operating in the MAT by the IT Support team. Decisions relating to access control and privilege are made by the Headteacher or their appointed deputy in the first instance and requests for alterations must be made to them in writing.

Section 10 Staff Devices

Staff issued laptops, iPads/iPhones, ID cards and fobs remain the property of the MAT and are issued to designated staff members for work use only. If the staff member or user leaves SHARE MAT employment or a loan period expires; the devices must be returned to IT Support for servicing and reassignment.





Staff devices are only to be used by the employee that the device is assigned to and must not at any time be shared or used by other staff or students. Devices should also not be used by friends or family members. Staff should not share the device's log in credentials or access PIN codes.

Under no circumstances should a member of MAT staff or any other unauthorised person attempt to repair or install software or hardware on devices. Any costs or damages arising from unauthorised repairs, software or hardware installation may be chargeable to the designated user.

Anti-virus software is installed on devices and will update automatically once the device is connected to the Internet.

MAT devices may be connected to home internet connections. It is not the responsibility of the MAT IT support staff to troubleshoot such use.

Any faults or problems with devices should be reported immediately to IT support.

Colleagues are advised to check car and home insurance policies to ensure they are adequately covered for any loss or damage prior to using device items at home.

Staff should ensure they do not leave devices in cars or permanently at home. They should be stored securely at all times.

Staff should take care when working in a public place, such as on a train, that their work is not visible to any other passengers.

iPads/iPhones

The iPad is a single-user device, which means it has a single login that is persistent. The single-user focus extends to apps like Safari, which keeps track of email logins, Microsoft Teams and web history for all users rather than a specific user. Staff must not share assigned iPads with others as it will compromise data-protection and security requirements. Student iPads are for student use only and a record of student use must be kept by staff.

Section 11 Remote/Home Working

A school issued mobile device will be provided to staff carrying out particular roles. These devices are prepared with a standardised image containing security configurations that must not be disabled. Staff in receipt of these devices must allow for critical and security updates to be completed.

Staff must take all precautions with the safety and security of mobile devices and will be required to sign an acceptable use form upon issue. Laptops are encrypted with BitLocker which will protect data on the laptop if it is lost or stolen.

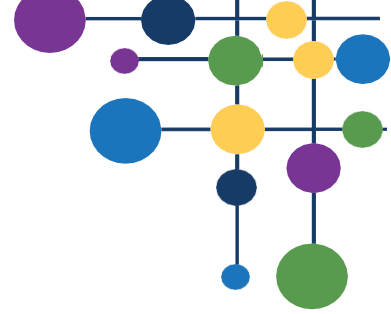
Staff must lock their screens if the device is left unattended, especially if there are children or others present. When the device is not being used it should be stored somewhere safe.

Staff must immediately report if the device is lost or stolen to the ICT Team and their line managers. Microsoft remote application to securely login onto site systems is provided. This system allows access to applications such as MIS. Details of login procedures and 'how to' guides can be found at <https://start.sharemat.org>.

Microsoft Office 365 login for Email, One-Drive, Teams is used and provided by Share Multi Academy Trust. Microsoft Office 365 is the Trust communication and secure remote file sharing service.

Staff are required to use Microsoft Office 365 services such as One-Drive and SharePoint to save/share data. On the recommendations of the NCSC, use of USB Flash drives is now being phased out as they pose a security threat and can easily be misplaced.





Staff are required to use the mobile device for work purposes only. Staff should take greater care in the use of the internet away from schools as they will not be protected to the same level of web filtering.

Share Multi Academy Trust uses Microsoft Intune as its Mobile Device Management (MDM) service. This gives the ICT Team the ability to enforce remote security compliance, remotely lock access and install critical configuration settings along with device location reporting.

All IT requests must be logged on the Every system. A link to this can be found at <https://start.sharemat.org>. Staff login using their Office 365 email account for single sign on.

All staff must undertake the cyber security threat training provided for greater understand of cyber threats and remote working.

Section 12 E-mail System

SHARE MAT encourages staff to send emails instead of letters, faxes and other forms of paper communications were deemed appropriate. This form of contact provides quicker communication and also a convenient way of filing such documents.

The email system should not be used as a means for sending unnecessary unsolicited emails, harassing groups or individuals or creating/continuing chain letters or spam. If an email is received that causes concern then a copy should be obtained where possible (either electronically or physically) and the IT Support team should be informed. The matter will then be investigated and action taken as appropriate.

All messages should have their content checked just as would be done for a physical document. Nothing should be sent in an email, especially to parents or contacts from outside of the MAT that would not be appropriate in a letter.

Care should always be taken before opening attachments, especially if they are from someone that you do not know or were not expecting an attachment from. The MAT's network will do checking and filtering of viruses from attachments but it is not possible to catch 100% of problems. If you suspect that an email or attachment contains a virus or has caused a problem, inform IT Support.

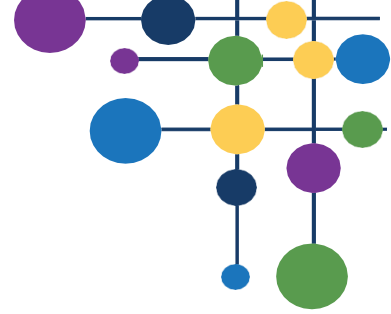
Staff and students should only use the MAT approved, secure email system(s) for MAT business. The MAT e-mail system(s) should not be used for personal use; similarly, personal accounts such as WhatsApp groups etc. should not be used for MAT business, a Teams chat should be setup instead and used for any work-related chat activities.

We also recognise that email has limitations; specifically, that it is often unable to reflect nuances in tone. For this reason, MAT staff will avoid using email for any communication which is likely to have emotional consequences for the sender or the recipient. In these cases, we will use face to face interaction.

Respect for others should be at the heart of all our communication. We will always try to think carefully before communicating. In addition, we will try our very best to do the following with regard to email:

- Ensure that every email is sent only to appropriate recipients.
- (Training will be provided to assist with the creation of distribution lists).
- Use the labels INFO (Information only – no action required by the recipient), ACT (Action of some kind will be required by the recipient) and CONF (the email is confidential and contains some sensitive information) to indicate the status of each email.
- Ensure that the subject heading contains an accurate summary of the email's contents.
- Avoid putting a student's name in a subject heading in order to prevent unnecessary embarrassment if the heading is inadvertently viewed by others.
- Do everything possible to avoid displaying email inadvertently.
 - Observe the norms of social communication such as greeting, signing off and spelling names correctly.



- 
- Carefully consider the use of CC. We will not use this to increase pressure on an individual. CC will only be used to copy in interested parties or relevant stakeholders.
 - Observe the following with regard to response time:
 - If a response is needed we will include a suggested response time in the email subject header. This would take the form ACT 06/10/14 for example. If all staff use this exact format, it means that anyone can search for a date and find out if anything needs to be done on that specific day. We may need to send a reminder to an individual who has not responded
 - Emails may be sent at any time convenient to the sender but no response will be expected outside normal working hours
 - We will respond to parental emails within 48 hours (Parents will be made aware of this through the Parent Bulletin)

Section 13 Use of the Internet and E-mail

Internet access will be available to staff and students via all workstations connected to the MAT's network and is for MAT and curriculum related purposes only.

All members of the MAT community and visitors to the MAT are expected to use the Internet in an appropriate manner at all times. Staff and students are expected to sensibly use the Internet.

The MAT has software systems that can monitor and record all internet usage, and record each chat, newsgroup or e-mail message. The MAT reserves the right to do this at any time. No user should have any expectation of privacy as to his or her internet usage.

The MAT reserves the right to inspect any and all files stored on the network in order to ensure compliance with MAT policies.

All use of the Internet by students, staff and other users will be monitored and users will be made aware of the monitoring procedure.

If students or staff discover unsuitable material the URL and the nature of the content should be reported immediately to IT Support. Any unsuitable URL or site deemed inappropriate by our Internet Service Provider will be automatically banned. SHARE MAT ICT staff will and are happy to ban or monitor sites at the request of staff. Requests to remove bans on sites should be directed to the IT Manager.

Any member of the MAT community or other MAT user who, in the opinion of the individual school Headteacher uses the Internet inappropriately will have their Internet access rights removed. The Headteacher may, in such cases, carry out disciplinary procedures.

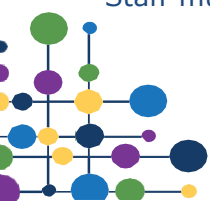
Where staff feel inappropriate sites, or material have been accessed, they should report it to IT Support.

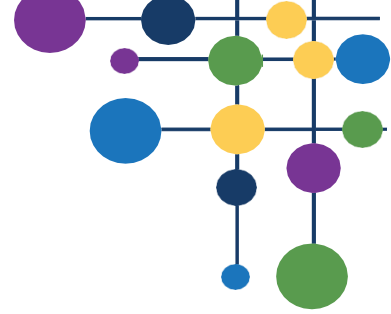
Staff should always report any accidental access to, or receipt of inappropriate materials, or filtering breach to the appropriate line manager or school named contact.

Staff must not allow unauthorised individuals to access email, Internet, Intranet, network, or other school or LA systems.

Offensive material should not be e-mailed. Anyone found doing this will be subject to severe disciplinary action. Staff will not engage in any online activity that may compromise professional responsibilities.

Staff must be aware of digital safeguarding issues so they are appropriately embedded in classroom practice.





No user may use the MAT's internet facilities to deliberately disable or overload any computer system or network, or to circumnavigate any system intended to protect the privacy or security of another user.

Section 14 Monitoring use of the Internet

SHARE MAT monitors usage of its internet, online content, online services and email services without prior notification or authorisation from users.

Users of SHARE MAT email and internet services should have no expectation of privacy in anything they create, store, send or receive using the MAT's ICT system.

Section 15 File Downloading

Any software or files downloaded via the Internet onto the MAT network become the property of the MAT.

Any such files or software may be used only in ways that are consistent with their licences or copyrights.

No user may use MAT facilities knowingly to download or distribute illegal software or data. The use of MAT resources for illegal activity will be grounds for immediate dismissal.

Any file that is downloaded must be scanned for viruses before it is run or accessed. No user may use the MAT Internet facilities to deliberately propagate any virus.

Video and audio streaming and downloading represent significant data traffic, which can cause local network congestion. Video and audio downloading are prohibited unless for agreed demonstration purposes.

Section 16 Chats and Newsgroups

Each user of the Internet facilities must identify him or herself honestly, accurately and completely (including MAT status and function if requested) when participating in chats or newsgroups, or when setting up accounts on outside computer systems.

Only those users who are duly authorised to speak to the media on behalf of SHARE MAT may speak or write in the name of the MAT to any newsgroup or web site.

Other users may participate in newsgroups or chats in the course of information research when relevant to their duties, but they do so as individuals, speaking only for themselves.

The MAT retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any employee in the course of his or her duties.

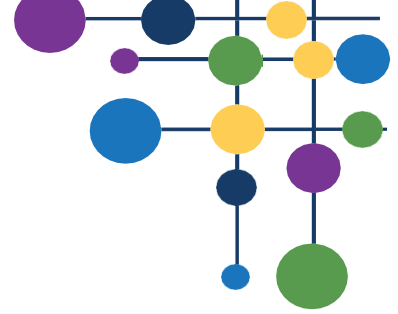
Users are reminded that chats and newsgroups are public forums and it is inappropriate to reveal confidential MAT information.

Section 17 Passwords

Any user who obtains a password or ID for an Internet resource must keep that password confidential. User IDs and passwords will help maintain individual accountability for Internet resource usage. The sharing of user IDs or passwords obtained for access to Internet sites is prohibited.

For staff passwords are required to be a minimum of 12 characters long containing uppercase, lowercase letters, numbers and symbols. Staff will be required to change this every 6 months, in line with NCSC guidelines.





Student passwords will be 10 characters long containing uppercase, lowercase letters, numbers and symbols. Students will be required to change this every 12 months. This password will then be used to access school devices and Microsoft 365 resources such as email and Teams.

Passwords must not be written down or shared with others.

Section 18 Security

The MAT has installed routers, firewalls, proxies, Internet address screening programmes, and other security systems to assure the safety and security of the MAT's networks. Any user who attempts to disable, defeat or circumvent any MAT security facility will be subject to disciplinary action.

Only those Internet services and functions, which have been documented for education purposes within the MAT, will be enabled at the Internet firewall.

Computers that use their own modems to create independent data connections sidestep our network security mechanisms. Therefore, any computer used for independent dial-up or leased-line connections to any outside computer or network must be physically isolated from the MAT's internal networks.

Personal use is permitted at the discretion of the MAT and can be limited or revoked at any time.

Internet of things or IOT devices such as games consoles, Amazon Echo etc. must not be connected to the trust's network as they cannot be secured and managed by the IT Team.

Section 19 Backing Up and Disaster Recovery

The IT Manager will ensure that regular and systematic back up of data is completed on a regular basis so that recovery of essential data can be managed in the event of loss of data files or system failure.

Backup copies will be securely stored against theft, corruption or physical damage so that in the event of a major incident a backup copy is available.

The MAT will ensure procedures are in place to recover all data and return ICT systems to full use in the event of a critical incident or local problem. RAID mirroring and virtual machine replication ensures data is not lost in the event of main server failure.

The IT Manager will maintain an up-to-date list of contacts that will be available to assist in the recovery process e.g., network management consultants, key staff, and suppliers.

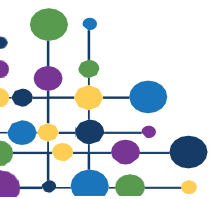
Section 20 Photographs and Photography

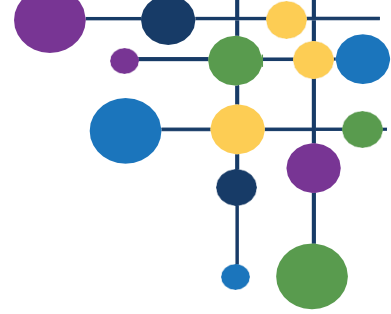
Photography in schools is subject to the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) regarding the rights of individuals to have information of a personal nature treated in an appropriate manner and the Human Rights Act 1998, protecting the privacy of individuals and families. As well as these statutory rights, restrictions on photography arise from issues of Safeguarding and Copyright in performances.

Photography includes photographic prints, streaming media and transparencies, video, film and digital imaging, created using devices such as cameras, video cameras, phones or tablets, etc.

Staff can be involved in the photography of students and staff for the following main purposes:

- Student administration
 - Curriculum or course work
 - EYFS Profile record keeping and evidence gathering
- Corporate and community activities.





When taking a picture, the MAT must obtain the consent of the person in the picture (for students over the age of 16) or their parent or carer for all other students.

Ensure that the commitment made in the consent form is followed:

- Not to name the student
- Not to use the photograph out of context
- Not to use the photograph to illustrate sensitive or negative issues.

When photographing students:

- Check parents/carers have given permission through the Consent Form. A list of students without Media Consent will be kept centrally at each individual school. It is each member of staff's responsibility to check this list if they intend to use any images of students.
- Ensure all students are appropriately dressed.
- Avoid photographs that only show a single child with no surrounding context of what they are learning or doing. A photograph for identification purposes may endure for several years but should not be retained when replaced or expired.
- Do not use images of a student who is considered vulnerable.
- Avoid naming students. If a name is required use only the first name.
- Use photographs that represent the diversity of the students participating.
- Report any concerns relating to any inappropriate or intrusive photography to the Designated Safeguarding Lead.
- Do not use any images that are likely to cause distress, upset or embarrassment.

Staff should use school equipment wherever possible for recording images of children. If exceptionally it is necessary for staff to use their own equipment (e.g. due to the malfunction of school equipment or an unexpected event) then the image should be handed to the school at the earliest opportunity and deleted from staff equipment, including mobile phones.

Section 21 Use of Digital Cameras

SHARE MAT is committed to utilising the latest technologies to support staff by making their teaching more effective and to help reduce staff administrative workload. All teaching/support staff are permitted to borrow digital cameras to aid in their duties.

The conditions for the use of digital cameras are set out below:

- All digital cameras will remain the property of SHARE MAT and will be returned to the MAT if employment should cease.
- Staff are responsible for ensuring that the camera is kept secure and will not be damaged.
- Staff will be trained in the use of digital camera and its computer software, dependent upon need.
- Staff will use the digital camera to aid their teaching and other activities related to the MAT
- The digital camera may not be used for any illegal or unprofessional activities.
- Any loss, damage or malfunction must be reported immediately.

Section 22 Social Media

The internet provides a range of social media tools that allow users to interact with one another. This policy sets out the principles that students, staff and governors are expected to follow when using social media.

It is crucial that all stakeholders in SHARE MAT, including students, parents, staff and the public at large have confidence in the MAT. The principles set out in this policy are designed



to ensure that the use of social media is responsibly undertaken and that confidentiality of students and staff and the reputation of the MAT are safeguarded.

All members of the MAT community must be conscious at all times of the need to keep their personal and professional lives separate.

MAT logos, crests, typefaces or brands must not be used or published on any personal web space or on any online or offline medium without prior consent (with the exception of identification of place of employment or sharing official MAT news feeds). These are registered trademarks, patents and the intellectual property of SHARE MAT.

This covers personal use of social media as well as the use of social media for official MAT purposes, including sites hosted and maintained on behalf of the MAT.

This policy applies to personal web space such as social networking sites (for example *Facebook*, *Instagram*, *Snapchat*), blogs, microblogs such as *WhatsApp*, *Twitter*, chatrooms, forums, podcasts, open access online encyclopaedias such as *Wikipedia*, social bookmarking sites such as *del.icio.us* and content sharing sites such as *Flickr* and *YouTube*.

The internet is a fast-moving technology and it is impossible to cover all circumstances or emerging media – the principles set out in this policy must be followed irrespective of the medium. Students should only use official school sites for communicating with staff, or with other students to communicate with one another for the purposes of an educational context.

Social media is an excellent means of communication for the trust and it is expected that the management of corporate social media will take place during the working day. The Headteacher has full responsibility for overseeing the individual school's official website, Facebook, LinkedIn, Flickr, Twitter and YouTube sites. No other social media platforms may be set up by any member of the whole school community which have a direct or indirect connection with SHARE MAT.

Whilst students and the wider school community are encouraged to interact with these social media sites they should do so with responsibility and respect.

Principles – Be responsible and Be Respectful

Users should be conscious at all times of the need to keep their personal and professional/school lives separate. They should not put themselves in a position where there is a conflict between the MAT and their personal interests;

Users should not engage in activities involving social media which might bring SHARE MAT or their own reputation into disrepute;

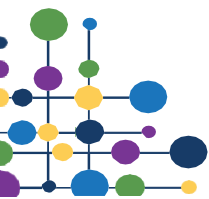
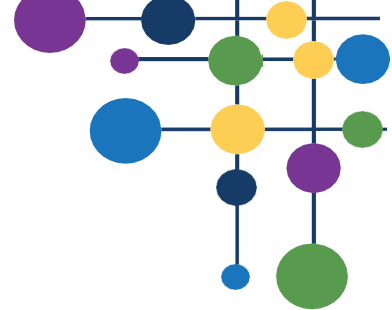
Users should not represent their personal views as those of SHARE MAT on any social medium;

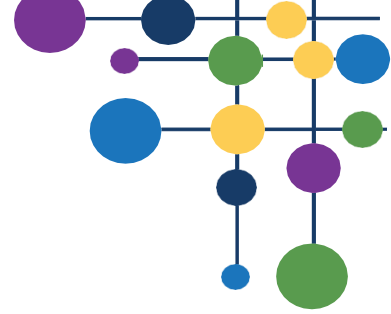
Users should not discuss personal information about other current or former employees or students at SHARE MAT and the wider community they interact with on any social media;

Users should not use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations or SHARE MAT;

Users are strongly advised not to publish their date of birth and home address on any social medium;

Users are strongly advised to think carefully about any photographs they appear in which other users could post on social medium.





Section 23 Personal Use of Social Media

Students, staff and governors should be careful when identifying themselves as members of SHARE MAT in their personal web-space. Consideration should be given to the type of information being linked with the MAT and to the safeguarding of the privacy of staff members, students and parents and the wider MAT community.

Staff members and governors should not have contact through any personal social medium with any students, past or present, up to the age of 18, (or 25 for vulnerable students) whether from SHARE MAT or any other school, other than those mediums approved by the Headteacher, unless the students concerned are family members.

If students wish to communicate with staff they should only do so through pre-approved school channels created officially for this purpose.

Information that students, staff and governors have access to as part of their involvement with SHARE MAT, including personal information, should not be discussed on their personal web space.

Photographs, videos or any other types of image of students and their families or images depicting staff members, clothing with MAT logos or images identifying MAT premises should not be published on personal or public web space without prior permission from the MAT.

MAT email addresses should not be used for setting up personal social media accounts or to communicate through such media. Students and staff should not manage their own personal media accounts during the working day.

Staff, students and governors should not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity. The source of the correction will be recorded and SHARE MAT reserves the right to amend these details for their sole purpose. All staff, students and Governors are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. All staff, students and governors should keep their passwords confidential, change them often and be careful about what is posted online.

Staff, students and governors should not post images or videos of staff or governors from MAT events on any public social media site without their prior consent.

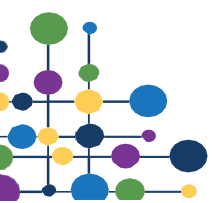
The MAT accepts that some sites may be used for professional purposes to highlight a personal profile with summarised details, e.g., LinkedIn. The MAT would advise that care is taken to maintain an up-to-date profile and a high level of presentation on such sites if SHARE MAT is listed.

Staff who run blogging/microblogging sites which have a professional and/or educational status are advised to seek guidance and advice from their Headteacher regarding prudence and endorsement of views if there is any link referencing SHARE MAT.

Cyber-Bullying

Cyber-bullying is defined as bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as mobile phones, computers, and tablets as well as communication tools including social media sites, text messages, chat and websites. Examples of cyber-bullying include abusive text messages or emails, rumours sent by email or posted on social networking sites, distributing embarrassing pictures, videos, websites or fake profiles.

Cyber-bullying by students and staff will not be tolerated and will be treated as seriously as any other type of bullying.



If a member of staff is aware of a bullying incident, they must take this seriously, act as quickly as possible to establish the facts and report the incident to the appropriate member of staff. These members of staff will investigate the matter fully, provide support for the victim, and alleged perpetrator (as appropriate) to act restoratively and apply consequences when necessary.

If a consequence is used, it will correlate to the seriousness of the incident and the bully will be told why it is being used. The student will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. The student may have their internet access suspended.

Any allegations of cyber-bullying by students will be managed in accordance with the Trust's Antbullying and Behaviour Policies.

If any member of staff is a victim of cyber-bullying they must report this behaviour as soon as possible to their line manager or the Headteacher. The victim will be offered support and this will be fully investigated and the relevant Trust policies followed, a referral may be made to the appropriate authorities if deemed appropriate.

Section 24 Mobile Phones and Personal Devices

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. There are issues surrounding student use of mobile phones to video and take photographs of other students and staff members for use in Cyberbullying. Devices with integrated cameras can lead to safeguarding, bullying and data protection issues. Mobile phones can also be used by students to access inappropriate internet material. If taken into the Trust school they can be a distraction in the classroom and are valuable items that could be stolen, damaged, or lost.

The Trust will not tolerate cyberbullying against either students or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will face consequences in accordance with the appropriate age-related Trust Behaviour and Anti-bullying policies.

Images or files should not be sent between mobile phones in the Trust school and mobile phones can be confiscated by a member of staff, and the device can be detained to be passed to police if there are concerns about harmful materials being stored on the device.

Any student who brings a mobile phone or personal device into the Trust school is agreeing that they are responsible for its safety. The Trust school will not take responsibility for personal devices that have been lost, stolen, or damaged.

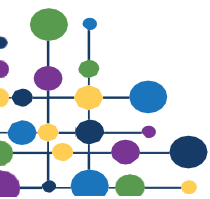
Students who breach the Behaviour or Anti-bullying Policies relating to the use of mobile phones and personal devices will be disciplined in line with these policies.

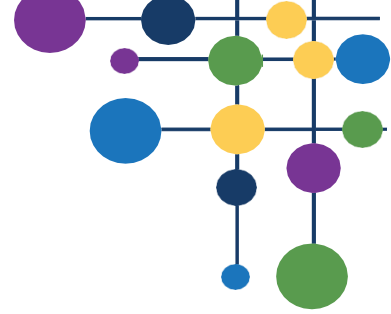
Staff using their own personal devices to access work documents/communication e.g. Teams, E-mail or One Drive, must adhere to the following guidance.

The personal device:

- Must have the latest security updates installed
- Must have a screen lock
- Must only be used by the trust staff member
- Should preferably have an antivirus software installed
- Must not be exposed to critical data

A function of Office 365 allows for trust management to remotely remove the application (Email/One Drive etc) from anyone who is a security concern and/or is in breach of the trust's ICT policy.





Section 25 Public Wi-fi Acceptable Use

Scope

This is applicable to all students, members of staff and visitors who connect or attempt to connect their electronic device to the MAT's public Wi-Fi networks.

Definitions

"Electronic Device"

Any electronic item fitted with a wireless transmitter. Including, but not limited to, any laptop, netbook, ultrabook, mobile phone, tablet and electronic reader.

"Public Wi-Fi Network"

Wireless infrastructure provisioned by the MAT at different sites to allow students, staff and visitors to the MAT to access an Internet connection on their own electronic devices. This is also known as 'BYOD' (Bring Your Own Device), and will allow different people to access the Wi-Fi at those sites that have it available.

Service Provision

ICT Helpdesk will help where possible with any queries regarding connection to their public Wi-Fi network. Support will **not** be provided for any other requests regarding personal electronic device's including, but not limited to software, hardware, maintenance, backup, data loss and file recovery. Users **must not** physically connect personal electronic devices to any MAT equipment.

MAT Visitor Usage

MAT visitors wishing to use any public Wi-Fi must be endorsed by a staff sponsor. The staff sponsor will contact IT Support to enable visitor usage. The sponsor's name will be held on record alongside the visitor's information.

Disclaimer

Connecting a personal electronic device to the MAT network is entirely at the users own risk. The MAT will NOT be liable for any (hardware or software) loss, damage, malfunctioning or inconvenience to your electronic device arising either directly or indirectly as a result of its connection to the public Wi-Fi networks. It is the user's responsibility to ensure that any software installed on their personal electronic device is correctly licensed.

Insurance

It is the user's responsibility to ensure that any electronic devices brought on to the MAT premises are suitably insured. The MAT's insurance **does not** cover personal electronic devices.

Health & Safety

Due to P.A.T. testing regulations users **must not** connect or charge their electronic device in school using a mains electricity outlet using personal equipment.

Connecting an electronic device to the public Wi-Fi networks

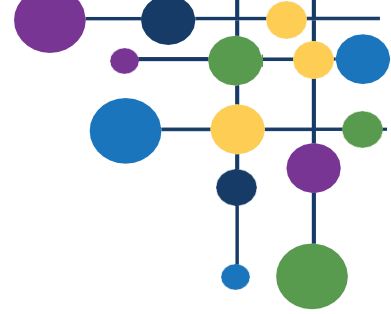
Note: The public Wi-Fi networks are for personal devices only. Users must not attempt to connect any MAT owned devices to them. All MAT owned devices already have Wi-Fi connectivity via a dedicated Wi-Fi network.

- Use of the Internet via the public Wi-Fi networks and a user's own electronic device is subject to the same conditions as set out in the appropriate Acceptable Use Policy section. Users must ensure that their Internet usage whilst connected to the public Wi-Fi networks are in line with these policies and appropriate within the MAT context.
- The public Wi-Fi networks are provided as an educational teaching and learning tool ONLY, and should only be used for this purpose.

Examples of activities **not** permitted whilst connected to the public Wi-Fi networks:

- Online gaming.
- Social networking.





- Peer-to-peer file sharing (including, but not limited to the use of torrents).
- Video and audio streaming of a non-educational nature.
- Using any form of 'proxy bypass' to bypass, or attempt to bypass, the MAT's Internet filtering system.
- Attempting to 'hack' or otherwise compromise the security and integrity of the public Wi-Fi networks.
- The use of 'tethering' to turn your electronic device into a Wi-Fi hotspot.
- Any personal downloads of a non-educational nature.
- Any other activity which results in a distraction from, or reduced performance in education / employment at the MAT.

This is **not** an exhaustive list.

Any passwords users are given to use in order to access the public Wi-Fi networks must be kept safe and secure at all times. Passwords must not be shared with anyone.

The public Wi-Fi networks provide an HTTP/HTTPS Internet connection only. They do not provide any other services.

In the interests of network performance, the MAT may restrict the data bandwidth and user experience to an individual user and electronic device, if it is deemed necessary.

As these are public Wi-Fi networks, they should be subject to the same precautions as any other open/public network. Users should ensure that their electronic device has suitable anti-virus and firewall security software installed, and that the network profile is set as 'public' or similar on the electronic device / firewall security software.

Privacy

Public Wi-Fi networks and Internet activity is logged and monitored at all times, in order for the MAT to meet with its Online Safety and Safeguarding responsibilities.

Withdrawal of Access

Access to the public Wi-Fi networks will be withdrawn with immediate effect if a user fails to adhere to this Acceptable Use Policy, or any other applicable MAT policy or guideline. Access to the public Wi-Fi networks may be restricted or withdrawn at any time, without notice, to ensure that the integrity and security of the network and/or other users are not compromised.

Section 26 Breaches

Any breach of this policy that leads to a breach of confidentiality, defamation or damage to the reputation of SHARE MAT or any illegal acts or acts that render SHARE MAT liable to third parties may result in legal action, disciplinary action or sanctions in line with the MAT policies for staff and students.

