INSPIRE

INCLUDE

INTEGRITY

EXCEED

Online Safety and Security Policy

Status	**Statutory**
Version	**7**
Responsible Directors' Board	**Finance and Operations Committee**
Responsible Persons	**Strategic Safeguarding Leader and Director of ICT**
Date Policy Reviewed	**September 2024**
Next Review Date	**September 2025**
Academy to implement without Amendment, using appendix when required	

Exceed Learning Partnership

• EVERY CHILD • EVERY CHANCE • EVERY DAY •

Summary of Changes from Previous Version

Version	Date	Author	Summary of Updates
V6	April 2024	Strategic Safeguarding Leader	Page 9 – reference made to additional policies: ELP Mobile Phones in Schools, Primary Policy and Hall Cross Academy Mobile Phone Policy Page 13 – updated to include: ***The use of portable removable storage such as USB drives or Mass Storage Devices is expressly forbidden within Exceed Learning Partnership and its Academies unless authorised by a member of the Academy Senior Management Team and authorised by the IT Department. Data should be stored to approved cloud-based storage such as Google Drive and accessed only by an ELP account.*** Page 19 – Updated to include obscene imagery made or edited using Artificial Intelligence
V7	July 2024	Strategic Safeguarding Leader	New section added – Section 2 – Legal framework Section 3 – Roles and responsibilities, subsection 'Principal and Senior Leaders'; phrase CEO/Principal changed to 'Principal of each academy' New section added – Section 15 – Generative artificial intelligence (AI)

Contents

1. Scope of the policy

This policy applies to all members of the Multi Academy Trust (MAT) community (including staff, pupils, volunteers, visitors) who have access to and are users of the ICT systems, both in and out of the MAT.

The Education and Inspections Act 2006 empowers the Principals of Academies within the MAT to such extent as is reasonable, to regulate the behaviour of pupils when they are off the Academy site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other Online Safety incidents covered by this policy, which may take place outside of the Academies, but is linked to membership of the Academy. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data

The Academies within the MAT will deal with such incidents within this policy and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of the Academy.

2. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'

- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2024) 'Keeping children safe in education 2024'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- ICT Acceptable Use Policy
- Cyber Response Policy Plan
- Child Protection and Safeguarding Policy
- Mobile Phones in Schools Policy (Primary)
- Mobile Phones in Schools Policy (Secondary)
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Confidentiality Policy
- Photography and Images Policy
- Device User Agreement
- Home and Remote Learning Policy

3. Roles and responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Trust and its academies:

Governors/Board of Directors

Governor and Directors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors/Directors receiving regular information about online safety incidents. *A member of the Governing Board and Directors will take on the role of Online Safety Governor (usually combined within the role of Safeguarding Governor) The role of the Online Safety Governor/Director will include:*

- *Regular meetings with the Online Safety Lead*
- *Regular monitoring of online safety incident logs*
- *Regular monitoring of filtering/change control logs*
- *Reporting to relevant Governor/Director meetings*

Principal and Senior Leaders

- The Principal of each academy has a duty of care for ensuring the safety (including online safety).
- The Principal of each academy and the Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse").
- The Principal of each academy is responsible for ensuring that the Online Safety Lead/Designated Safeguarding Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Principal of each academy and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in the MAT who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

Designated Safeguarding Lead – (Online Safety Lead)

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the Trusts online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the MAT/Local Authority
- liaises with MAT technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Meets regularly with the Online Safety Governor/Director to discuss current issues, review incident logs and filtering/change control logs
- Attends relevant meetings of Governors/Directors
- Reports regularly to the Senior Leadership Team
- Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
  - sharing of personal data
  - access to illegal/inappropriate materials ○ inappropriate on-line contact with adults/strangers ○ potential or actual incidents of grooming ○ cyber-bullying

Director of ICT/ICT Technical Support staff:

The Director of ICT & Technical Support Staff are responsible for ensuring:

- that the MAT's technical infrastructure is secure and is not open to misuse or malicious attack
- that the MAT meets required online safety technical requirements
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering system, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the network/ internet/remote access/email is monitored in order that any misuse/attempted misuse can be reported to the CEO/Principal /Designated Safeguarding Lead for investigation /action /sanction
- That monitoring software/systems are implemented and updated.

Teaching and Support Staff

Are responsible for ensuring that**:**

- they have an up to date awareness of online safety matters and of the current Trust/academy online safety policy and practices
- they have read, understood and signed the staff acceptable use policy/agreement
- they report any suspected misuse or problem to the CEO/Principal/Senior Leader/Safeguarding Lead for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official Academy systems
- online safety issues are embedded in all aspects of the curriculum and other activity
- pupils understand and follow the Online Safety Policy and acceptable use policies.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other Academy activities (where allowed) and implement current policies with regard to these devices
- In lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Pupils

- are responsible for using the Trust /academy digital technology systems in accordance with the pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the take/use of images and online-bulling
- should understand the importance of adopting good online safety practice when using digital technologies out of the Trust/Academy if related to the membership of the Academy

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The Trust/Academy will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and social media.
Parents/carers will be encouraged to support the Academy in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at Academy events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records

Community Users

Community users who access Academy systems or programmes as part of the wider Academy provision will be expected to sign a Community user Acceptable Use Agreement before being provided with access to Academy systems.

4. Policy statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the Academies within the MAT's online safety provision. Children and young people need the help and support of the MAT/Academy to recognise and avoid online safety risks and build their resilience.

In planning their online safety curriculum Academies within the Trust may wish to refer to:

- DfE Teaching Online Safety in Academies
- Education for Connected Word Framework
- SWGfL Barefoot Computing Project – online safety curriculum programme and resources

Online Safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum, should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside the Trust and its academies.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such

a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – Parents/Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The Trust and its academies will therefore seek to provide information and awareness to parents/carers through

- Curriculum activities
- Letters, newsletters, website, Learning Platforms
- Parent/carers information sessions
- High profile events/campaigns
- Reference to the relevant web sites/publications e.g. https://swagfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the Trust's Online Safety Policy.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Designated Safeguarding Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The Designated Safeguarding Lead will provide advice/guidance/training to individuals as required.

Training – Directors & Governors

Directors and Governors should take part in online safety training /awareness sessions with particular importance for those who are members of any group involved in technology/online safety/health and safety/safeguarding. This may be offered in a number of ways: This may be offered in a number of ways:

- Attendance at training provided by the Local Authority /MAT/National Governors Association or other relevant organisation
- Participation in MAT information sessions for staff/parents

Technical – infrastructure / equipment, filtering and monitoring

The Director of ICT will be responsible for ensuring that the MAT infrastructure / network is as safe and secure as is reasonably possible and that procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- MAT technical systems will be managed in ways that ensure that they meet recommended technical requirements
- There will be regular reviews of the safety and security of MAT technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to MAT technical systems and devices.
- All users will be provided with a username and secure password by the academy Business Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- The "master / administrator" passwords for the MAT ICT system, used by the Network Manager must also be available to the CEO/Principal and kept in a secure place (e.g.
  safe)
- The Business Manager within each academy is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- **Internet access is filtered for all users**. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list.
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet.
- MAT technical staff are able to monitor and record the activity of users on the MAT technical systems and users are made aware of this.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the MAT systems and data. These are tested regularly. The MAT infrastructure and individual workstations are protected by up to date virus software.
- Each Academy has Sophos Central Anti-Virus with Intercept X in place specifically designed to target malware and ransomware threats
- The Academy has provided enhanced/differentiated user-level filtering
- The use of removable media (e.g. memory sticks/CD/DVDs is not permitted by users on trust devices. Personal data cannot be sent over the internet or taken off the Trust/academy site unless safely encrypted or otherwise secured.
- An agreed policy in in place for the provision of temporary access of guests (e.g. trainee teachers, supply teachers, visitors) onto the Academy systems.
- An agreed policy is in place regarding the extent of personal use that users and their family members are allowed on Academy devices that may be used out of Academy
- An agreed policy is in place that allows/forbids staff from downloading executable files and installing programmes on Academy devices.

5. Mobile technologies

Mobile technology devices may be MAT provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the MAT's wireless network. The device then has access to the wider internet which may include the Academies learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile/personal devices in a MAT context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the MAT's Online Safety education programme.

- The Trust and its academies technical systems will be managed in ways that ensure that the trust and its academies meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of technical systems within the Trust and its academies.
  Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to the technical systems and devices within the trust and its academies
- All users are asked to sign an acceptable user agreement prior to receiving devices

The MAT allows:

	Academy Devices		Personal Devices		
	MAT owned for single user	**MAT owned for multiple users**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in the MAT	Yes	Yes	No	Yes	Yes
Full network access	Yes	Yes	No	No	No
Internet only				Yes	Yes
No network access					

MAT provided devices:

- Can be used in or out of the MAT for the business of the MAT
- Personal use is allowed
- The management of the devices/installation of apps/changing of settings is the responsibility of the MAT
- Network/broadband capacity is the responsibility of the MAT
- Technical support is provided by the MAT

- Filtering of devices is provided by the MAT
- Access to cloud services is provided by the MAT where appropriate
- Data Protection is the responsibility of the user
- Taking/storage/use of images is the responsibility of the user
- All devices will be returned to the MAT should the user leave the employment of the MAT
- Any damage is to be reported to the MAT
- Staff training is provided by the MAT

Personal devices:

Staff who use a personal device should refer to the additional ELP policies (depending on the setting they are in):

ELP Mobile Phones in School Primary Policy

Or

Hall Cross Academy Mobile Phone Policy

- Personal mobile devices can be brought into the MAT
- Staff will be allowed to use personal devices for MAT business should no other devices be made available to them
- Network/broadband capacity is the responsibility of the user
- Technical support is the responsibility of the user
- Filtering of the internet connection to these devices is the responsibility of the user
- Personal devices should not be used for sensitive MAT data which might breach Data Protection regulations
- The MAT has the right to take, examine and search users devices in the case of misuse
- Taking/storage/use of MAT images of pupils or staff without their consent is not permitted
- Liability for loss/damage or malfunction is the user's responsibility
- Data Protection is the responsibility of the user
- Users must be made aware that the MAT has the right to take, examine and search users' devices in the case of misuse (must be included in the behaviour policy)

6. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and instant use of images that they have recorded themselves or downloaded from the internet. However, staff need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The MAT will inform and educate users about these risks:

- When using digital images, staff should be aware and inform and educate pupils of the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents/carers will be obtained before photographs of pupils are published on the academy/trust websites/social media/local press.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Academy policies concerning the sharing, distribution and publication of those images. Those images should only be taken on MAT equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the MAT into disrepute.
  Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at Academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

7. Data protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The MAT must ensure that:

- It has a Data Protection Policy
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.

- It has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- It has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- It has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a procedure for reporting, logging, managing, investigating and learning from information risk incidents.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data

  There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- can recognise a possible breach, understand the need for urgency and know who to report it to within the Academy
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the Academy

When personal data is stored on any portable computer system:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete

The use of portable removable storage such as USB drives or Mass Storage Devices is expressly forbidden within Exceed Learning Partnership and its Academies unless authorised by a member of the Academy Senior Management Team and authorised by the IT Department. Data should be stored to approved cloud-based storage such as Google Drive and accessed only by an ELP account.

8. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the Academies currently consider the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults		
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff
Mobile phones may be brought to the MAT	x		
Use of mobile phones in social time	x		
Taking photos on mobile phones / cameras			
Use of other mobile devices e.g. tablets	x		
Use of personal email addresses in MAT, or on MAT network			
Use of MAT email for personal emails		x	
Use of messaging apps	x		
Use of social media			x
Use of blogs			x

When using communication technologies, the MAT considers the following as good practice:

- The official MAT email service may be regarded as safe but not secure and can be monitored. Users should be aware that email communications can be monitored.
- Users must immediately report, to the nominated person, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff that is MAT related i.e. emails must be professional in tone and content. These communications may only take place on official MAT systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Personal information should not be posted on any MAT material and only official email addresses should be used to identify members of staff.

9. Social media – protecting professional identity

All Academies and Local Authorities have a duty of care to provide a safe learning environment for pupils and staff. The MAT could be held responsible, indirectly for acts of its employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the MAT liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

The MAT provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the MAT through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
- Insurance protection to cover the costs of restoring and protecting data in the event of a cyber-attack on the network

MAT staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or MAT staff
- They do not engage in online discussion on personal matters relating to members of the MAT community
- Personal opinions should not be attributed to the MAT
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official MAT social media accounts are established there should be:

- A process for approval by the CEO
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including:
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under MAT disciplinary procedures

Personal Use:

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with the MAT or impacts on the MAT, it must be made clear that the member of staff is not communicating on behalf of the MAT with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the MAT are outside the scope of this policy
- Where excessive personal use of social media in the MAT is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The MAT permits reasonable and appropriate access to private social media sites **Monitoring of Public Social Media:**

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the MAT
- The MAT should effectively respond to social media comments made by others

10. Unsuitable / inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from MAT and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a MAT context, because of the nature of those activities.

The MAT believes that the activities referred to in the following section would be inappropriate in a MAT context and that users, as defined below, should not engage in these activities in/or outside the MAT when using MAT equipment or systems. The MAT policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments	that contain or relate to:	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
		Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
		Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
		Pornography				X	
		Promotion of any kind of discrimination				X	
		threatening behaviour, including promotion of physical violence or mental harm				X	
		Promotion of extremism or terrorism				X	
		Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the MAT or brings the MAT into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to Academy networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)							x
Using Academy systems to run a private business						X	

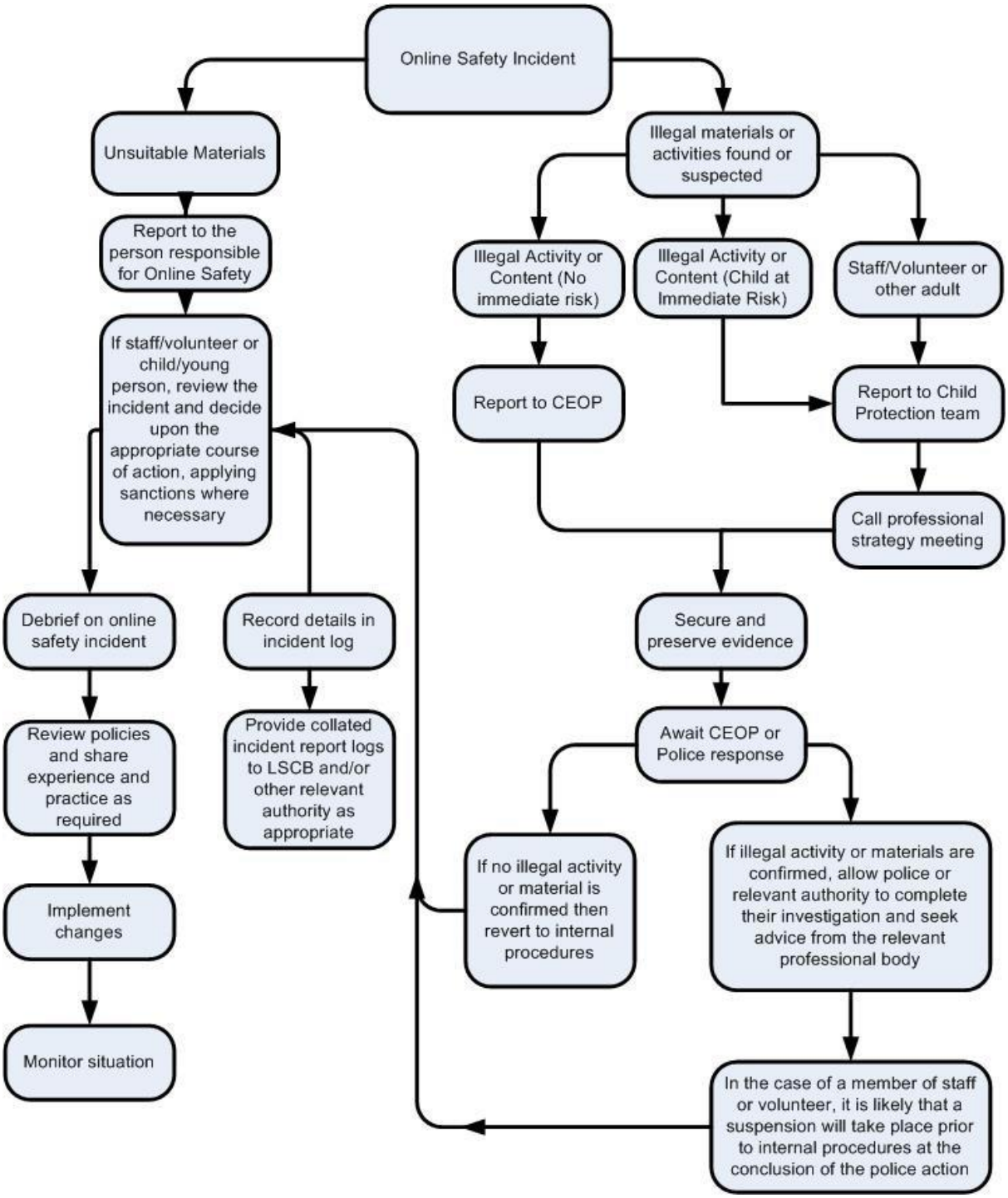
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the Trust/ academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)				x	
On-line gaming (non-educational)				x	
On-line gambling				x	
On-line shopping / commerce		x			
File sharing		x			
Use of social media		x			
Use of messaging apps		x			
Use of video broadcasting e.g. YouTube		x			

11. Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

12. Illegal incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



13. Other incidents

It is hoped that all members of the MAT community will be responsible users of digital technologies, who understand and follow the MAT policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated it will need to be judged whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:

- incidents of 'grooming' behaviour ○ the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act (this can include images generated or edited using Artificial Intelligence)
- criminally racist material ○ promotion of terrorism or extremism ○ other criminal conduct, activity or materials
- offences under the Computer Misuse Act (see Users Actions chart above)

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the MAT and possibly the Police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained for evidence and reference purposes.

14. MAT actions & sanctions

It is more likely that the MAT will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the MAT community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Staff Incidents	Refer to line manager	Refer to CEO/ Principal	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X				x
Inappropriate personal use of the internet/social media / personal email	x						
Unauthorised downloading or uploading of files	x						
Allowing others to access MAT network by sharing username and passwords or attempting to access or accessing the MAT network, using another person's account	x						
Careless use of personal data e.g. holding or transferring data in an insecure manner	x						
Deliberate actions to breach data protection or network security rules		x					
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x					
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x					
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		x					
Actions which could compromise the staff member's professional standing		x					
Actions which could bring the MAT into disrepute or breach the integrity of the ethos of the MAT		x					
Using proxy sites or other means to subvert the MAT's filtering system		x					

Accidentally accessing offensive or pornographic material and failing to report the incident		x					
Deliberately accessing or trying to access offensive or pornographic material		x					
Breaching copyright or licensing regulations		x					
Continued infringements of the above, following previous warnings or sanctions		x					x

15. Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

Policy reviewed September 2024

Signed B.A. Nixon

CEO:

Signed:
Chair of Directors:

Policy to be reviewed: September 2025