Online Safety
Policy & Procedure

Thornhill Community Academy

MAT Version	5.0
Name of Policy writer	Jenny Carr
Last review date	September 2025
Next review due date	October 2027
Approved by Directors	9th October 2025

Schedule of amendments:
v4.0 – addition of paragraphs to address the risks, benefits and safe practices around the use of AI
V5.0 – updated to reflect KCSIE 2025

Contents

Section 1: Policy Statement

SHARE MAT is committed to keeping our pupils as safe as possible, both in school and beyond. Pupils are exposed to risks online and this policy describes the steps we will take to try to reduce these risks and help prevent children from suffering harm. It contains specific procedures and guidance to complement our Safeguarding and Child Protection Policy.

Unsafe online practices may lead to pupils coming to harm. It is therefore vitally important staff and others recognise the signs of abuse, as well as understanding how to reduce the risks. These signs can be found in our Safeguarding and Child Protection Policy and publications such as Keeping Children Safe in Education 2025.

Online Safety covers the use of the internet as well as mobile phones, electronic communications technologies and the use of social media and social networks.

The Trust recognises that online systems and mobile technology can be an important tool for aiding communication, development of social skills and teaching and learning. The use of online systems and mobile technology to interact socially and share ideas can benefit students, staff and parents/carers; however, it is important that the use of the internet and internet enabled devices is seen as a significant responsibility for students, staff and parents/carers, that must be used appropriately.

Section 2: Scope

It is essential that all students, staff and parents/carers in all Academies are alert to online safety and the possible risks when using the internet and internet enabled devices. Possible risks to online safety can arise from the misuse of the following to harm children and young people:

- Mobile phones/mobile devices
- The internet
- Chat rooms/gaming sites
- Social networks

The harm might range from:

- Sending abusive texts and emails
- Harassment and stalking behaviour
- Coercing children and young people to engage in sexually harmful conversations or actions online; such as webcam filming, sending explicit photographs, or arranging face-to-face meetings.
- This can also lead to blackmail, sharing of inappropriate images, and child exploitation, both sexual and criminal.

It is also important that students, staff and parents/carers are aware of the importance of responsible conduct online.

Section 3: Legal and Statutory framework

Academies will fulfil their local and national responsibilities as laid out in the following documents:

- The most recent version of Working Together to Safeguard Children (DfE)
- The most recent version of Keeping children safe in education - GOV.UK
- Sharing nudes and semi-nudes: how to respond to an incident (overview) - GOV.UK (www.gov.uk)
- Safeguarding children and protecting professionals in early years settings: online safety considerations for managers - GOV.UK (www.gov.uk)
- Mental health and behaviour in schools (publishing.service.gov.uk)
- Preventing and tackling bullying (publishing.service.gov.uk) and cyber-bullying: advice for headteachers and School staff
- Teaching about relationships, sex and health - GOV.UK (www.gov.uk)
- Relationships education, relationships and sex education (RSE) and health education
- Voyeurism offences act 2019
- Teaching online safety in Schools
- Preventing and tackling bullying
- Cyber-bullying: advice for headteachers and School staff
- Searching, screening and confiscation at school
- The DfE's guidance on protecting children from radicalisation: the prevent duty.

The policy also takes into account the National Curriculum computing programmes of study.

Section 4: Policy aims and objectives

Share MAT Academies will:

- Have robust processes in place to help protect the safety of pupils, staff, volunteers and governors when working online, whether they are using the trust's networks or other technology in our academies
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole Academy community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Educate our pupils, staff, trustees and parents, to help them to stay safe online
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** ––being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

The 4 categories of risk outlined above determine our staff training and PSHE curriculum, to ensure all staff and pupils have the knowledge and understanding to reduce their risks online.

Section 5: Roles and Responsibilities

5.1 The board of directors

The board has overall responsibility for monitoring this policy and holding the trust leaders to account for its implementation.

The directors who oversee online safety are ~~Richard Amos~~ and Mark Day.

All directors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on the Share MAT ICT Policy
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

5.2 The local governing body

Check the policy is being implemented fully, is well understood in school and risks are being managed well. They must report any concerns to the board.

The governing body should co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

5.3 The Chief Executive Officer

Is responsible for checking the policy is being implemented fully across the trust and reporting any concerns to the board. The CEO must intervene if there are weaknesses in an academy's practice.

5.4 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the Academy.

5.5 The Designated Safeguarding Lead

Details of the academy's DSL [and deputy/deputies] duties are set out in the Share MAT Safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in the Academy, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the Academy
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the Academy's Safeguarding policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the Academy behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary

- Providing regular reports on online safety in the Academy to the headteacher and/or governing board
- Reviewing any web filtering system alerts identified by the trust's ICT technicians, and the monitoring and filtering identified by Smoothwall Monitor, to determine whether further action is necessary
- Raise awareness via training and information to staff, pupils and parents of the benefits and risks associated with Artificial Intelligence (AI), including deep fakes, privacy and safety.

This list is not intended to be exhaustive.

5.6 The Trust ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online whilst working in the trust, including terrorist and extremist material
- Ensuring that the trust's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the trust's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy's behaviour policy
- Refer any concerns to the DSL
- Provide guidance on the safe and effective use of AI across the trust for all stakeholders.

This list is not intended to be exhaustive.

5.7 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on the Share MAT ICT Policy and ensuring that pupils follow the Academy's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'
- Use AI in line with trust guidance.

This list is not intended to be exhaustive.

5.8 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms of the Academy's ICT Policy, Behaviour Policy and Acceptable Use (of ICT) agreement with the Home / School agreement.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- National Online Safety: Webinars and courses for parents to increase knowledge of Internet Safety. The Academy will issue log in details for this website.
- Common Sense Media: Independent reviews, age ratings and other information about all types of media for children and their parents
- support for parents and carers to keep children safe online - GOV.UK (www.gov.uk): Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Information, Advice and Support to Keep Children Safe Online (internetmatters.org): age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Parents and Carers | Safer Internet Centre: Tips, advice and guides to keep children safe online
- Stop It Now! UK and Ireland | Preventing child sexual abuse: Can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- Educate Against Hate - Prevent Radicalisation & Extremism: provides advice for parents and carers to keep children safe from online radicalization.

5.9 Visitors and members of the community

Visitors and members of the community who use the Academy's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Section 6: Procedures and implementation: Educating pupils about online safety

All Academies have to teach:

- Relationships education and health education in primary Academies
- Relationships and sex education and health education in secondary Academies.

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns.

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including prison
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- How to identify if online material is expressing extremist views how to protect themselves and their peers from radicalisation.

All Academies:

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Educating parents about online safety

The Academy will raise parents' awareness of internet safety in letters or other communications home, and in information via the Academy website. This policy will also be shared with parents. Please also see useful websites for parents in section 3.8 of this policy.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the Academy's behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The Academy will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups. Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The Academy also sends information on cyber-bullying to parents via letters and the Academy website, so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the Academy will follow the processes set out in the Academy behaviour and Safeguarding policies. Where illegal, inappropriate or harmful material has been spread among pupils, the Academy will use all reasonable endeavours to ensure the incident is contained and will contact external agencies, where required.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the Academy rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of Academy discipline), and/or
- Report it to the police*.

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the Academy complaints procedure.

The Prevent Duty

The Academy/Trust works to ensure pupils are safe from terrorist and extremist material when accessing the internet. Appropriate levels of filtering are in place through a managed filtering service which includes terms related to terrorism. Appropriate monitoring of internet use, in the academy will identify attempts to access such material. Pupils are educated to evaluate information accessed with a reporting procedure that identifies inappropriate sites so that action, including blocking, can be put into place.

Acceptable use of the internet in the Academy

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the Academy's ICT systems and the internet. Visitors will be expected to read and agree to the Academy's terms on acceptable use if relevant.

Use of the Academy's internet (including Wi-fi) must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites (including those accessed by mobile devices connected to the academy wi-fi) visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils using mobile devices in the Academy

Pupils may bring mobile devices into the Academy, but are not permitted to use them during:

- Lessons
- Form time
- In the Corridors.

Any use of mobile devices in the Academy by pupils must be in line with the Share MAT ICT Policy.

Any breach of acceptable use by a pupil may trigger disciplinary action in line with the Academy behaviour policy, which may result in the confiscation of their device.

Section 7. Monitoring and evaluation: How the Academy will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet (or ICT and the Internet outside of school, which leads to health and safety risks for themselves or others) we will follow the procedures set out in the Academy Behaviour and ICT policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Filtering and Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Stakeholder	Roles and responsibilities
Trust Directors / Central Team	Promote a strong commitment to safeguarding by checking the training and system compliance. Annual policy review and updates.
Governors	Reports from school leaders on the filtering and monitoring trends and how the system is improving safety for all.
ICT Team	Ensure the ICT monitoring and filtering systems are installed and DSL's (and other assigned staff) receive the pupil alerts. Ensure that the ICT monitoring and filtering systems, ensure that the Headteacher receive staff based alerts. Review filtering and monitoring provision at least annually. Block harmful and inappropriate content without unreasonably impacting teaching and learning. Have effective monitoring strategies in place that meet their safeguarding needs. Use the 'plan technology for your school service' to self assess the trust against the filtering and monitoring standards. Use the generative AI in education guidance to inform best practice.
Headteacher	Receives the staff alerts. Investigates, records, liaises with appropriate stakeholders and actions next steps.
SLT	Receive termly updates on number of alerts trends and key risks. Are alerted to concerns and amend curriculum/ interventions accordingly. Headteacher at their designated school to receive alerts that are staff based from ICT.
DSL	Receive all pupil alerts. Check that alert have been investigated, recorded on CPMOS and actioned correctly. Share information on new emerging trends /themes to SLT and PD lead. Keeps staff training up to date with latest online safety concerns/risks.
Head of Year	Receives the pupil alerts for the year group. Investigates, records on CPOMS, liaises with appropriate stakeholders and actions next steps.
Members of staff	Reads the policy. Completes all mandatory training. Follows the acceptable use policy.
Pupils	Follows the acceptable use policy. Educated via lessons and assemblies on how to safely use the internet.
Parents/carers	Signposted to the acceptable use policy for students and the systems in place to support online behaviour.

	Signposted to guidance on online use, NOS support for various platforms. Ensures appropriate measures are in place at home and on mobile devices. Promotes internet safety within the home.

(See flowchart in appendix 1)

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. Further details are provided in the trust's ICT policy.

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.

Section 8. Training and awareness

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including child on child abuse (including sharing of nude/semi-nude images, upskirting and cyber-bullying) and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). All Early Career Teachers and Trainees will also receive appropriate training, as will long-term supply staff or other contractors.

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL [and deputy/deputies] will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in the Share MAT Safeguarding Policy.

Section 9. Links with other policies

This online safety policy is linked to the following policies:

- Share MAT Safeguarding policy
- Academy Behaviour policy
- Share MAT ICT policy
- Academy Anti-bullying policy.

Appendix 1: Online Safety Flowchart

This flowchart should be used by staff to determine, the course of action following concerns about Online Safety of students.

Route A

Has a student reported to you that they have:

- Sent or received **comments**
- Sent, received or viewed **content or images**

of a bullying/sexual harassment/sexual/discriminative/ extremist nature

↓

Staff member to record concerns on CPOMS

A DSL will then complete an investigation, including the collection of statements and taking photos of any evidence.

DSL will liaise with the Share MAT IT Support Team, where appropriate.

Route B

Have you found or seen inappropriate material being viewed/sent or suspect that it has been viewed/sent **on a portable device e.g. smartphone?**

↓

Staff member to confiscate the device and inform a DSL to view the images/content

Staff member to record the incident on CPOMS

A DSL will then complete an investigation, including the collection of statements and taking photos of any evidence.

DSL will liaise with the Share MAT IT Support Team, where appropriate.

Route C

Have you found inappropriate material, seen inappropriate material being viewed/sent or suspect that it has been viewed/sent **on a Share MAT PC/laptop or other device?**

↓

Staff member to confiscate the device/ isolate the student from the PC.

If the machine is in use, the staff member is to contact itsupport@sharemat.co.uk and the DSL immediately

Staff member to record the incident on CPOMS

A DSL will then complete an investigation, including the collection of statements and taking photos of any evidence.

Appendix 2: Filtering and Monitoring Flowchart

Head of Year and DSL receive pupil online safety alerts via email and CPOMS alert tray

Head of Year checks the alert

Questions to consider:

- Is this child at significant risk of harm? If so, act immediately.
- Is this a result of curriculum work that was being completed?
- How does the child explain how the alert came about?
- Is this the first alert / do any other concerns exist (check CPOMS)?
- Do you need to alert the DSL to the outcome of the fact find?

Does a safeguarding concern exist?

NO

The alert is a false positive e.g., searching for a hotel for a curriculum subject. No safeguarding context.

No recording / action required

Remind the pupils of why we safeguard them by using filtering systems.

YES

What level of concern does this represent?

Do you need to alert the DSL immediately?

Have you communicated the concern and follow up with the parent/carer?

Have you asked the child what support they need?

Have you identified the best support for the child? (Intervention/risk assessment/referral to an external agency)?

Have you explained why we safeguard them in this way?

Recording the alert and actions:

- Log the action on CPOMS following the alert
- Record conversation with pupil
- Record evidence from subject (e.g. – it was in a X lesson and matches the curriculum content)
- Record any details of any stakeholders that have been contacted
- Have you decided the level of action that is required. *(Levels – reminder of the password / computer safety rules/ small group support with a particular safeguarding theme / 1:1 support with a particular safeguarding theme/ referral to an external organisation)*
- Have you signposted to helpful information?
- Record any actions/follow up required