East Midlands Academy Trust

Online Safety Policy

'Every child deserves to be the best they can be'

Inclusion Innovation Impact

Scope: East Midlands Academy Trust & Academies within the Trust	
Version: V2	**Filename:** EMAT Online Safety Policy
Approval: October 2025	**Next Review:** October 2026 This Policy will be reviewed every two years by the Owner and approved by the Trust Board
Owner: Head of Shared Services	

Revision History

Revision Date	Revisor	Description of Revision
September 2025 v2	DU	Complete re-write of policy to reflect the centralised nature of EMAT and to reference the Trusts Safeguarding lead

1. Aims

East Midlands Academy Trust (EMAT) aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, governors, members and Trustees
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- 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, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- 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 the user 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 scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also considers the National Curriculum computing programmes of study.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

In this policy the term 'School Leader' applies to the individual registered with the Department for Education as Headteacher / Principal of the school.

3.1 The Trust Board and Local Advisory Board (LAB)

The Trust Board has overall responsibility for monitoring this policy and holding the CEO to account for its implementation.

The LAB will make sure all academy staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The LAB will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The LAB will ensure the that school leaders co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The LAB will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The Trust Board will make sure that the Trust has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the Trust in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the Trust's safeguarding needs

All Trustees and LAB members will:

- Make sure they have read and understand this policy
- Agree and adhere to the Trust's acceptable use policy

- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school / Trust approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is 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.

3.2 Trust Leadership

Trust Leadership is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the Trusts schools and central office.

3.3 The Trusts designated safeguarding lead.

Details of the Trust's designated safeguarding leads are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The Trust's designated safeguarding lead takes lead responsibility for online safety within EMAT:

- Supporting the Trusts leadership in making sure that staff understand this policy and that it is being implemented consistently throughout the Trust
- Working with the Trust leadership ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place in Trust schools.
- Providing the Trust Board assurance that filtering and monitoring systems are working effectively and reviewed at least annual.
- Working with the Trusts IT department to make sure the appropriate systems and processes are in place.
- Working with Trust leadership, the Trusts IT department, and other staff, as necessary, to address any online safety issues or incidents.
- Supporting school DSLs to ensure that all online safety issues and incidents are managed in line with their school's child protection policy
- Ensuring school-based DSLs are responding to safeguarding concerns identified by filtering and monitoring.
- Making sure that any online safeguarding incidents are logged and dealt with appropriately in line with the Trusts safeguarding policy.
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with EMAT's behaviour policy.
- Liaising with other agencies and/or external services if necessary

- Provide annual reports on online safety in the Trust to the governing board.
- Undertaking annual risk assessments that consider and reflect the risks pupils face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

3.4 IT Business Partner

The IT Business Partner is responsible for:

- Recommending and putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on Trust devices and Trust networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Making sure that the Trust's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Liaising with other agencies and/or external services if necessary
- Ensuring all EMAT staff undertake their mandatory Online Safety training on an annual basis.
- Conducting a full security check and monitoring the Trust's ICT systems on an annual basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the EMAT's or its academies behaviour policies.
- Knowing that the Trust's Data Protection lead is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by following the Trust's Cyber Security Incident Response Plan (CSIRP)

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Understanding of this policy
- Following the correct procedures by contacting the Trust's safeguarding lead if they need to bypass the filtering and monitoring systems for educational purposes

- Working with the Trust's safeguarding lead to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the Trust or it's academies school behaviour policies
- 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'
- This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the School Leader of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to Trusts acceptable use policy

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

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

3.7 Visitors and members of the community

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

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

All schools must teach:

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

In Key Stage (KS) 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private.
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

Pupils in Key Stage (KS) 2 will be taught to:

- Use technology safely, respectfully, and responsibly.
- Recognise acceptable and unacceptable behaviour.
- Identify a range of ways to report concerns about content and contact.
- Be discerning in evaluating digital content.

By the end of primary school, pupils will know:

- That the internet can be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others, including when we are anonymous.
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data are shared and used online
- How to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted.
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know.
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- Why social media, computer games and online gaming have age restrictions and how to manage common difficulties encountered online.
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- Where and how to report concerns and get support with issues online.

In KS3, 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 KS4 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 that 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 that carries severe penalties including jail.
- 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)
- The similarities and differences between the online world and the physical world, including: the impact of unhealthy or obsessive comparison with others online (including through setting unrealistic expectations for body image), how people may curate a specific image of their life online, over-reliance on online relationships including social media, the risks related to online gambling including the accumulation of debt, how advertising and information is targeted at them and how to be a discerning consumer of information online.

5. Educating parents/carers about online safety

EMAT schools will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website This policy will also be published on the online.

Online safety will also be covered during parents' evenings.

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with their School Leader and/or their school's DSL.

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

6. 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 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

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

EMAT schools will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

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.

EMAT schools also sends information/leaflets on cyber-bullying to parents/carers so 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, EMAT schools will follow the processes set out in their school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained and notify external law enforcement agencies as required under uk law.

School based DSLs will report the any incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so. The Trusts IT Department will also provide any expert support as required.

6.3 Examining electronic devices

The Trust IT Department or any member of staff authorised to do so by the Trust leadership, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the Trust rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Trust leadership, Trust IT department and or Trust safeguarding lead.
- Explain to the pupil why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Trust safeguarding lead and Trust leadership to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

Illegal material will not be deleted or erased unless approved to do so by law enforcement agencies, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the Trust safeguarding lead immediately, who will decide what to do next. The Trust safeguarding lead will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening 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 Trust's complaints procedure.

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.

EMAT recognises that AI has many uses to help pupils learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

EMAT will treat any use of AI to bully pupils very seriously, in line with the Trusts behaviour policies

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by EAMT, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of AI should be in accordance with EMAT's AI policy.

7. How the school will respond to issues of misuse

Where a pupil misuses the Trusts ICT systems or internet, we will follow the procedures set out in our policies on Behaviour and Acceptable Use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the Trust's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct, acceptable use policy and staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

EMAT will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

8. Training

8.1 Staff, LAB Members, Trustees, Members and Volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including 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).

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, threatening, 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 up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The Trust Safeguarding lead and school based DSL's and DDSL 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.

The Local Advisory Board and Trust Board 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 our child protection and safeguarding policy.

8.2 Pupils

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

9. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT acceptable use policy