

East Midlands Academy Trust

Online Safety Policy 2023/2025

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

Scope: East Midlands Academy Trust & Academies within the Trust	
Version: V2	Filename: EMAT Online Safety Policy
Approval: Feb 2023 <i>Approved by the Trust Board</i>	Next Review: March 2025 <i>This Policy will be reviewed by the Trust Board (FHRE committee) every two years</i>
Owner: East Midlands Academy Trust Board of Trustees	Union Status: Not Applicable

Policy type:	
Non-Statutory	Replaces Academy's current policy

Revision History

RevisionDate	Revisor	Description of Revision
February 2022	DU	Policy update – no changes

EMAT Online Safety Policy

1. Aims

East Midlands Academy Trust (EMAT) aims to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in the Trust's activities.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on [preventing and tackling bullying](#) and [searching, screening and confiscation](#). It also refers to the Department'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.

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

3. We believe that:

- children and young people should never experience abuse of any kind
- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

4. We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using EMAT's network and devices

- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

5. We will seek to keep children and young people safe by:

- appointing an online safety coordinator. This will be the Head of Safeguarding & Inclusion.
- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents/carers (*appendix 2*)
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person (*see appendix 1*)
- reviewing and updating the security of our information systems regularly
- ensuring that usernames, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

6. If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account (*see appendix 1*)
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

7. Training

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).

The DSL and 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.

Trustees 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. Review and Monitoring

The board of Trustees has overall responsibility for monitoring this policy and holding the CEO to account for its implementation. This policy will be monitored by the LAB as part of the academy's annual internal review and reviewed by the trustees on a two-year cycle or as required by legislation changes.

The Local Advisory Board will monitor the implementation of this policy in schools by liaising with the Headteacher and the Designated Safeguarding Lead.

9. Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Child protection and Safeguarding Policy
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- IT Acceptable Usage Policy
- Behaviour Policy
- Anti-bullying Policy

Appendix 1 – Response to incidents of inappropriate online behaviour

Where a pupil misuses the Trust’s ICT systems or internet, the school will follow the procedures set out in the Behaviour policy. 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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

IT Based Safeguarding Systems

Website Blacklisting : The blocking of access to unacceptable websites (blacklisting) for anyone connected to any trust network is controlled through a Cisco Meraki firewall device.

- In Primary schools this is a [Meraki MX 84](#)
- In Secondary schools this is a [Meraki MX100](#)

In addition, all of these devices have been installed with [the Advanced Security License](#)

These devices are fully equipped with latest software updates and maintained centrally by the ICT team. Changes to the firewall’s blacklisting settings must be approved by the Head of Shared Service and would only happen after consultation and approval from Head of Safeguarding and Inclusion

Monitoring of Safeguarding Key Words

The monitoring of keywords being typed into student and staff devices is carried out by a product called [Senso](#).

Any incidents occurring in schools will be dealt in the first instance by the DSL who will assess the context and determine whether the incident is a legitimate concern that might require further action.