East Midlands Academy Trust

Online Safety Policy 2021/2023

‘Every child deserves to be the best they can be’

East Midlands Academy Trust is a company limited by guarantee registered in England & Wales No. 08149829
Orchard Academy, Shepherdswell Academy, Castle Academy, Hardingstone Academy, Stimpson Avenue Academy,
Prince William School and Northampton International Academy are all business names of the East Midlands Academy Trust.

Scope: East Midlands Academy Trust & Academies within the Trust	
Version: V1	**Filename:** EMAT Online Safety Policy
Approval: March 2021 *Approved by the Trust Board*	**Next Review: March 2023** *This Policy will be reviewed by the Trust Board (FHRE committee) every two years*
Owner: East Midlands Academy Trust Board of Trustees	**Union Status:** Not Applicable

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

EMAT Online Safety Policy

1. Aims

East Midlands Academy Trust 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 [name of organisation]'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 and 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 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
- 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 ofthe 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 equiped 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.

Appendix 2 –

Responsible Use of Internet

As part of the pupils' curriculum enhancement and the development of ICT schools, Castle Academy is providing supervised access to the internet including email.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home, and we enclose references to information on safe internet access that may be of use.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the school cannot be held responsible for the nature or content of materials accessed through the Internet. The school will not be liable under any circumstances for any damages arising from your child's use of the Internet facilities.

I enclose a copy of the rules for responsible Internet use that we operate at Castle Academy.

Should you wish to discuss any aspect of internet use please speak to the Head of School.

To enable your child/ren to use the internet and email during lesson times please complete and return the attached permission slip.

Permission for Internet Access

Parent/Carers Permission	**Pupil's agreement**
I give permission for access to the internet on the terms set out in the above letter.	I agree to follow the rules for responsible internet use
Signed…………………… **Print……………………** **Date…………………………**	**Signed……………………………** **Print……………………………** **Date………………………………**

Acceptable Internet Use Statement

The computer system is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration, and management. The school's internet access policy has been drawn up to protect all parties – the students, the staff, and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any interest sites visited.

- Access must be only made via the authorised account and password, which must not be made available to any other person.
- All interest use should be appropriate to staff professional activity or students' education.
- Activity that threatens the integrity of the school ICT systems, or that attacks or corrupts other systems, is forbidden.
- Sites and materials accessed must be appropriate to work in the school. Users will recognise materials that are inappropriate and should expect to have their access removed.
- Users are responsible for e-mail they send and for contacts made that may result in email being received.
- The same professional levels for language and content should be applied as for letters or other media, particularly as email is often forwarded.
- Posting anonymous messages and forwarding chain letters is forbidden.
- Copyright of materials and intellectual property rights must be respected.
- Legitimate private interests may be followed, providing the school is not compromised.
- Use for personal gain, gambling, political purposed or advertising is forbidden.

Rules for Responsible Internet Use

The school has installed networked computers and internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will ask permission from a member of staff before using the internet.
- I will not access other people's files.
- I will use the computers only for schoolwork and homework;
- I will not bring floppy disks into school.
- I will only email people I know, or my teacher has approved.
- The messages I send will be polite and sensible.
- I will not give my home address or phone number, or arrange to meet someone, unless my parent, carer or teacher has given permission.
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or receive messages I do not like.
- I understand that the school may check my computer files and may monitor the internet sites I visit.