Eastington Primary School Filtering and Monitoring Policy

(To be applied with related policies for Safeguarding and Child Protection Policy, Online Safety and Acceptable Use Policy, Behaviour Policy and Anti- Bullying and Harassment Policy and Safer Working Practices Policy).

This policy reflects the statutory guidance 'Keeping Children Safe in Education' from the DfE September 2024 and the Filtering and Monitoring Standards for Schools and Colleges from the DFE January 2024. It is reviewed annually in line with an audit of provision.

Created - May 2024
Reviewed – September 2024
Next review – September 2025

This policy is based on the Department for Education (DFE's) Filtering and Monitoring Standards for Schools and Colleges and the statutory safeguarding guidance: Keeping Children Safe in Education 2023, Annex C, and its advice for schools about: Teaching Online Safety in Schools, Preventing and Tackling Bullying, Cyber-Bullying. Advice for Headteachers and School Staff, Searching, Screening and Confiscation and advice published by the UK Council for Online Safety.

Aims

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers the school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- Content: being exposed to illegal, inappropriate, or harmful material; for example, pornography, fake news, racist or radical and extremist views.
- Contact: being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images, or online bullying.

Roles and Responsibilities

The Governing Body

The Governing Body has overall responsibility for monitoring this policy.

The Governing Body will co-ordinate meetings with the appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
- Ensure that online safety is a running and interrelated theme while devising and implementing the whole school approach to safeguarding and related policies and/or procedures.
- Ensure 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.

The Headteacher

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

The Designated Safeguarding Lead

- The DSL takes lead responsibility for online safety in school, in particular;
- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, ICT technician and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.
- Ensuring that any online safety incidents are logged (on CPOMS e.g. an adult noting a child searching for something inappropriate online) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged (on CPOMS) and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.

The ICT Technician

The ICT Technician 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 while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems provide a high level of security and protection (no system can be 100% failsafe) against viruses and malware, and that such safety mechanisms are updated regularly and monitoring the school's ICT systems on a monthly basis.
- Maintaining systems used for blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

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 of the school's Online safety and Acceptable Use Policy.
- Working with the DSL to ensure 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 school 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'.

All staff are aware of reporting mechanisms for safeguarding and technical concerns. They should report if:

- they witness or suspect unsuitable material has been accessed.
- they can access unsuitable material.
- they are teaching topics which could create unusual activity on the filtering logs.
- there is failure in the software or abuse of the system.
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks.
- they notice abbreviations or misspellings that allow access to restricted material.

Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Understand that their child has read, understood, and agreed to the terms of the school's Appropriate 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
Hot topics – Childnet International
Parent resource sheet – Childnet International

Visitors and Members of the Community

Visitors and members of the community who use the school'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 of the Online Safety and Acceptable Use Policy.

Filtering and Monitoring

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

At this school, the web filtering software used is RM SafetyNet Primary, this system is used to protect over a million children in the UK. At Eastington Primary School, we have decided that the below options are the most appropriate because they will ensure that pupils can only access websites available through the school network (subject to filters set up) with the additional monitoring provided by adults in the classroom throughout any

online activities. Whilst pupils use the iPads or laptops and are accessing online content, adults will walk around the classroom to monitor their activities.

There are two types of appropriate monitoring used in school:

1. Physical monitoring (adult supervision in the classroom).
2. Web search monitoring provided by: RM SafetyNet Primary - Reports

The ICT technician makes monthly checks on the web search reports and produces and shares a report with the DSL and Headteacher. Filtering and monitoring procedures for the school are reviewed annually.
If concerns are raised by the web search report(s) e.g. searches for self- harm, SLT will work with staff to identify the child. This would involve logging children's use of IT equipment.

Further information can be found on the following websites: www.thinkuknow.co.uk
www.disrespectnobody.co.uk www.saferinternet.org.uk www.internetmatters.org
www.childnet.com/cyberbullying-guidance www.pshe-association.org.uk
http://educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-onlineradicalisation www.gov.uk/UKCCIS
https://www.rm.com/products/rm-safetynet