Mehria Primary School

E-Safety Policy

<u>Date agreed: September 2025</u>

<u>Review date: September 2026</u>

<u>(Sooner if required)</u>

Signed:___Zia Qazi______________________

Head Teacher

Signed:__Steven Odd______________________

Chair of Governors

1. Policy Statement

Mehria Primary School recognises that the internet and digital technologies are essential tools in 21st-century education. They offer huge opportunities for learning, communication, and creativity but also present significant safeguarding challenges.

This policy aims to:

- Protect pupils, staff, and the school community from online harm.
- Promote the safe, responsible, and respectful use of technology.
- Equip children with the resilience and critical thinking skills to navigate the online world.
- 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

Online safety is not just an ICT issue but an integral part of the school’s safeguarding and child protection framework.

---

2. Scope

This policy applies to:

- All pupils on roll
- All school employees (teaching, support, volunteers)
- Governors and trustees
- Parents and carers
- Visitors, contractors, and anyone else using the school’s ICT systems

It covers:

- Use of the internet, school networks, and school devices
- Use of personal devices (e.g., smartphones, tablets) when on school premises or accessing school systems
- Use of digital platforms for communication, homework, or remote learning

---

3. Legal and Statutory Framework

This policy is written in line with:

- Keeping Children Safe in Education (KCSIE) 2025
- Education Act 2002
- Data Protection Act 2018 / UK GDPR
- Prevent Duty Guidance 2015 (revised)
- Malicious Communications Act 1988
- Communications Act 2003
- Sexual Offences Act 2003
- Children and Families Act 2014
- Children's Wellbeing and Schools Bill (2025)

---

4. The Four Cs of Online Risk

Mehria Primary School addresses risks within the **Four Cs** model:

1. **Content** – exposure to illegal, harmful, or age-inappropriate material, including violent content, pornography, hate speech, extremist ideology, misinformation, disinformation, conspiracy theories, and harmful health advice.
2. **Contact** – harmful online interaction with others, including grooming, sexual exploitation, bullying, coercion, radicalisation, or impersonation.
3. **Conduct** – children's own behaviour online, including bullying, sexting, oversharing personal data, and engaging in risky challenges.
4. **Commerce** – financial and commercial risks, including scams, gambling, in-app purchases, and advertising.

---

5. Roles and Responsibilities

Governing Body

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 their whole school or college 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

- Do all that they reasonably can to limit children's exposure to the risks identified in the 4C's from the school's IT system. The governing body will ensure their school has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They will ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.
- The governing body will consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

Headteacher

- Ensures online safety is a school-wide priority.
- Allocates resources to maintain secure systems and staff training.

Designated Safeguarding Lead (DSL) – Zile Humm

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy. 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 manager and other staff, as necessary, to address any online safety issues or incidents
- Working with the headteacher, ICT manager and other staff, as necessary, to ensure the appropriate filtering and monitoring systems are in place and reviewed regularly
- Managing all online safety issues and incidents in line with the school child protection and safeguarding policy
- Ensuring that any online safety incidents are logged in line with the child protection and safeguarding policy (cause for concern forms)
- Ensuring that any incidents of cyber-bullying are logged 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
- Providing regular reports on online safety in school to the headteacher and/or governing board

All Staff and Volunteer

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 acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged in line with the child protection and safeguarding policy (cause for concern forms)

- 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’

  This list is not intended to be exhaustive.

Pupils

- Follow the Pupil Acceptable Use Agreement.
- Report anything online that makes them feel worried or uncomfortable.
- Treat others with respect online.

Parents & Carers

- Support the school’s approach to online safety.
- Engage with school-provided resources and guidance.
- Monitor children’s online activity at home.

---

6. Education and Curriculum

Online safety is embedded into teaching across subjects and year groups. It is explicitly taught in:

- **Computing** – safe internet use, passwords, privacy settings, recognising scams.
- **PSHE / RSE** – healthy online relationships, consent, managing emotions, digital wellbeing.
- **Assemblies & Theme Days** – e.g., Safer Internet Day, Anti-Bullying Week.

Pupils learn to:

- Recognise and report harmful content and contact.
- Critically assess information and spot fake news.
- Understand online reputation and digital footprints.
- Navigate social media responsibly (age-appropriately).
- Protect personal data and privacy.

In Key Stage 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 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

By the end of primary school, pupils will know:

- 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 online 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 is shared and used online 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 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.

7. Cyber-bullying

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.

Types of cyber bullying may include:

- Child on child sexual abuse and harassment
- Threatening, facilitating or encouraging sexual violence.
- Upskirting, i.e. taking a picture underneath a person’s clothing without consent and with the intention of viewing their genitals, breasts or buttocks. Sexualised online bullying, e.g. sexual jokes or taunts.
- Unwanted and unsolicited sexual comments and messages.
- Consensual or non-consensual sharing of sexualised imagery.
- Abuse between young people in intimate relationships online).
- Grooming and exploitation Where an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing.

Child sexual exploitation (CSE) and child criminal exploitation (CCE):

CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed

online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.
CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet. Radicalisation, the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Online hoaxes and harmful online challenges:

An online hoax is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms. harmful online challenges refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same.
An online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Preventing and addressing cyber-bullying:

Mehria has a zero tolerance approach to any forms of 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 school 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.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the 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. The DSL will report the 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.

8. Examining electronic devices :

The headteacher, and any member of staff authorised to do so by the headteacher, 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 school 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 headteacher.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, 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 headteacher 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.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence.

In these instances, they will not delete the material, 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 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 DSL immediately, who will decide what to do next.

The DSL 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

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school’s terms of acceptable use. Work devices must be used solely for work activities. If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

---

9. Filtering and Monitoring

- The school uses **age-appropriate filtering and monitoring software** to block harmful content and detect risk indicators.
- Filtering settings are reviewed annually and when needed.
- Changes to filtering require DSL authorisation.
- Monitoring alerts are reviewed promptly by the DSL or a delegated safeguarding-trained staff member.
- Logs of changes and alerts are retained in line with data protection laws.

---

10. Use of Technology

- Staff must only use school-approved platforms and devices for communication with pupils.

- Personal devices should not be used to contact pupils or store their personal information.
- Images and videos of pupils must follow the school's data protection and consent procedures.
- Social media use by staff must not compromise professional standards.

---

11. Managing Online Safety Incidents

All incidents are treated as safeguarding matters and managed according to the **Child Protection Policy**.
Types of incidents include:

- Cyberbullying
- Grooming / online exploitation
- Sexting / sharing of sexual images
- Extremist or radicalising content
- Financial scams
- Breaches of Acceptable Use Agreements

Incident Response:

1. Record on the safeguarding system immediately.
2. Inform the DSL.
3. DSL investigates and determines next steps (including contacting parents, police, or other agencies).
4. Support offered to victims and, where appropriate, those responsible for harm.

---

12. Staff Training

- All staff and governors receive online safety training at induction and annually thereafter.
- DSLs receive advanced training to understand emerging risks (e.g., AI-generated content, deep fakes).
- Training covers the Four Cs, incident handling, filtering and monitoring, and curriculum delivery.
- Misinformation, disinformation and Conspiracy theories under the content section of four 'C's.

---

13. Parental Engagement

The school will:

- Host annual online safety workshops for parents/carers.
- Share regular guidance via newsletters, the website, and social media.

14. Data Protection

Online safety measures will comply with the UK GDPR and Data Protection Act 2018. Personal information will only be collected, stored, and shared when lawful and necessary.

15. Policy Review

- This policy will be reviewed annually by the DSL and ratified by the Governing Body.
- It may be updated sooner in response to statutory changes, new threats, or significant incidents.