Thomas Telford Multi Academy Trust

Online Safety Policy

Redhill Primary Academy

and

Thomas Telford Primary Free School

Signed

Mrs Raj Samra
Chair of Governors
September 2026

It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate. (KCSIE, 2026)

At Redhill Primary Academy and Thomas Telford Primary Free School, we aim to ensure all groups of pupils are safe and feel safe at all times. We want our children to understand what constitutes unsafe situations and be aware of how they can keep themselves and others safe in different situations, including in relation to online safety. The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Our schools' online safety policy helps to ensure safe and appropriate use.

Through our policy for online safety, we aim to achieve the following:

- To protect and educate pupils and staff in their use of technology;
- To ensure that the schools provide a broad and balanced online safety curriculum;
- To ensure that the schools have the appropriate mechanisms to monitor incidents and ensure they are recorded and dealt with accordingly;
- To ensure pupils are fully aware of cyber-bullying and can actively try to prevent it from occurring;
- To engage and inform parents and the wider school community in order to ensure that children are safe online when at home.

What is the role of the online safety coordinator?

As online safety is an important aspect of strategic leadership within the schools, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named online safety coordinator in Redhill Primary Academy is **Amy Coughlan** and at Thomas Telford Primary Free School it is **Heidi Taylor**. All members of the school community have been made aware of who holds these posts.

The online safety co-ordinator should carry out the following:

- Remain actively aware of current issues and guidance through organisations such as CEOP and 'Think U Know'.
- Take day-to-day responsibility for online safety issues and have a leading role in establishing and reviewing the schools' online safety policy and associated documents.

- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place. (Record on CPOMS and tag as 'ESafety' so that the online safety coordinator is notified.)
- Provide training and advice for staff regularly through email, bulletins (Mail on Friday) and staff meetings.
- Receive reports of online safety incidents and create a log of incidents to inform future online safety developments.
- Liaise regularly with Governors to discuss current issues, review incident logs and filtering / change control logs.
- Lead the online safety pupil group.
- Provide training materials and advice for parents, ensuring that they know where to get help and support. For example, with harmful online challenges and hoaxes.
- Carry out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face.

Other roles and responsibilities

Governors

- Governing bodies and proprietors should ensure that all governors and trustees receive appropriate safeguarding and child protection (including online) training at induction.
- Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports.
- Governors will ensure that filtering and monitoring systems are reviewed and documented at least annually. The review will involve the DSL, the member of SLT responsible for filtering and monitoring (the headteacher) and the Trust's IT support provider. Governors will receive assurance that filtering and monitoring systems are effective and appropriate for the age range and safeguarding risks within the school, being careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.
- Whilst all children should be protected, it is important that governing bodies and proprietors recognise that some groups of children, are potentially at greater risk of harm than others (both online and offline). The list below, is not exhaustive, but highlights some of those groups.
  - Children who need a social worker
  - Children who are absent from education
  - Children who are home educated
  - Children requiring mental health support
  - Looked after and previously looked after children
  - Children with SEND or health issues
  - Children who are lesbian, gay, bisexual or gender questioning

Headteacher and Senior Leaders

- The Headteacher is responsible for ensuring the safety (including online safety) of all members of the school community.
- The Headteacher and Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- Ensure that all staff within the schools receive appropriate online safety training, including an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- Recognises that cyber security is a safeguarding issue. Appropriate measures will be taken to protect personal data, secure user accounts, prevent unauthorised access; reduce vulnerability to phishing and cyber-attacks and protect pupils from harms arising from data breaches.

Technical support staff

Technical support staff should ensure the following:

- The schools' ICT infrastructure is secure and is not open to misuse or malicious attack.
- Users may only access the schools' networks through a properly enforced password protection policy, in which passwords are regularly changed.
- The use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the online safety coordinator.
- Monitoring software / systems are implemented and updated as agreed in school policies.

Teaching and support staff

Teaching and support staff should ensure the following:

- Exercise professional curiosity, understanding that children can be at risk of harm online, and that abuse can take place wholly online, or technology may be used to facilitate offline abuse.
- Understand that children can abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography to those who do not want to receive such content.
- Recognise that children are also increasingly being targeted and recruited online using social media. Children can easily become trapped by this type of exploitation as county lines gangs can manufacture drug debts which need to be worked off or threaten serious violence and kidnap towards victims (and their families) if they attempt to leave the county lines network.
- They have an up-to-date awareness of online safety matters and of the current schools' online safety policy and practices.
- They have read, understood and signed the schools' Staff Acceptable Use Policy / Agreement (AUP).
- Any suspected misuse or problems detected are reported to the online safety coordinator, computing coordinator or other member of the Senior Leadership Team.

- Digital communications with pupils (e.g. homework on Microsoft Teams) should be on a professional level and only carried out using official school systems.
- Online safety issues are embedded in all aspects of the curriculum and other school activities.
- Pupils understand and follow the schools' online safety policy.
- ICT activity in lessons, extra-curricular and extended school activities are closely monitored.
- In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- New staff receive information on the schools' acceptable use policy as part of their induction as well as a breakdown of systems from the relevant people.
- They are aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.
- Incorporate online safety activities and awareness within their curriculum areas.

Designated Safeguarding Lead

The schools' Designated Safeguarding Lead should be trained in online safety issues and be aware of the potential for serious child protection issues to arise from the following:

- sharing of personal data.
- access to illegal / inappropriate materials.
- inappropriate on-line contact with adults / strangers.
- potential or actual incidents of grooming.
- cyber-bullying.

Pupils

All pupils at Redhill Primary Academy and Thomas Telford Primary Free School should ensure the following:

- Use the schools' ICT systems in accordance with the age-specific Pupil Acceptable Use Policies, which they are expected to sign at the beginning of each school year during the first block of computing teaching.
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying.
- Understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the schools' online safety policy covers their actions out of school, if related to their membership of the school.
- If staff or students discover an unsuitable site, the monitor must be switched off/ closed and the incident reported immediately to the online safety co-ordinator or teacher as appropriate.
- To safeguard and protect pupils, smart watches are **not** allowed to be worn at school due to the functions pupils would have to film, take photographs, record conversations and access social networking sites.

- The online safety pupil group learn about issues and look at training their peers in how to behave safely whilst online.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children.

We believe that it is essential for parents / carers to be fully involved with promoting online safety both in and outside of school and also to be aware of their responsibilities. We regularly consult and discuss online safety with parents / carers and seek to promote a wide understanding of the benefits related to ICT and associated risks. Information relating to online safety will be disseminated to parents when appropriate through the following channels: information evenings, letters, posters, the schools' website and the schools' newsletter.

Parents and carers will be responsible for the following:

- Parents / carers are asked to read the age-specific acceptable use policies on their child's admission to Redhill or Thomas Telford Primary and annually thereafter. (These will be sent home at the beginning of each academic year at the request of the online safety coordinator via the schools' office.)
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken / used in the public domain (e.g. on the schools' websites).

What dangers could children face online?

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate, or harmful content, for example: AI-generated harmful content, deepfake imagery, pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes and interactions with AI chatbots or virtual assistants.
- **Conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, 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), creation and sharing of AI-generated images, misuse of generative AI tools and online bullying.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing, cryptocurrency scams AI-enhanced fraud and financial scams.

At Redhill Primary Academy, how do we minimise online risk for our children?

Content	School uses KidRex as a search engine and higher up in school, children are taught how to use Google safely. Children are taught how to identify inappropriate information, close the page and report to an adult. All internet activity is monitored and inappropriate use or searches are captured by Policy Central.
Contact	Children are taught about 'stranger danger' online and progress to learning about risks such as grooming, stalking and being involved in groups that may be detrimental to well-being. **Also see below: *How is social networking managed at Redhill Primary Academy?***
Conduct	Children are taught the consequences of unwanted or illegal conduct online. Children are taught about the causes and effects of cyber-bullying as well as the consequences if found to be a participant or actor. Children and parents are regularly updated and informed about the risks associated with the overuse of technology. **Also see below: *How is social networking managed at Redhill Primary Academy?***
Commerce	Children are taught about the importance of strong passwords, misinformation, disinformation, online scams (including features to look out for e.g. URL shorteners, personality tests, red open padlock symbols, spelling/grammar errors)

How is cyber-bullying dealt with at Redhill Primary Academy and Thomas Telford Primary Free School?

Cyber-bullying, or online bullying, can be defined as the use of technologies by an individual or by a group of people to deliberately and repeatedly upset someone else. Cyber-bullying is a form of child-on-child abuse and can often linked to discrimination, including on the basis of gender, race, faith, sexual orientation, gender identity or special educational needs and disabilities. Incidents for cyber-bullying will be dealt with the by the online safety co-ordinator and a DSL if required. We will follow our child-on-child abuse policy in consultation with our relationships and behaviour policy when dealing with incidents of cyber-bullying. As soon as an incident has been reported or identified, the child will receive appropriate support and school will do all they can to stop the incident from spreading and assist in removing material from circulation. We will also work with the person who has carried out the bullying to ensure that it does not happen again. Some cyber-bullying content and activity is illegal. If a child is under the age of 18, it is illegal for them to make, possess or distribute any inappropriate explicit imagery of someone under the age of 18 which is 'indecent'. Young people who share sexual imagery of themselves, or peers, are breaking the law. Incidents involving a child producing sexual imagery will be treated as a safeguarding issue and the Designated Safeguarding Lead in school will deal with the incident. Where the police are notified of a

child under the age of 18 who is in possession of an indecent image or has been sending or taking these types of photos, they are obliged, under the Home Office Counting Rules and National Crime Recording Standards, to record the incident on their crimes system. This includes 'upskirting.'

How do we ensure that children with SEND access the internet safely and appropriately?

- Designated Safeguarding Leads [DSLs] are trained to recognise the additional risks that children with SEND face online e.g. cyber-bullying, grooming and radicalisation.
- All staff are acutely aware of vulnerable children (including but not limited to those with SEND) in their classes. If there is an online safety concern that is child-specific, class teachers would seek advice from both the SENDCO and online safety coordinator (DSL) in school.
- We try to avoid the use of abstract language and concepts to minimise confusion and misunderstandings. Through our progressive scheme of work (Project Evolve) we build and develop a collaborative understanding of the terminology being used around online safety. This is checked upon through our regular pupil voice interviews which always involve a diverse sample of pupils.
- Our online safety rules are clear, concise and not left open to interpretation. They are also differentiated for the younger and older children in school.
- During our parent consultations for children with SEND, we share our online safety rules with parents if appropriate to ensure that rules and consequences are consistent at school and home. At this point, any child-specific advice or strategies are shared with parents.
- Children's online safety education is based on their needs and experiences. Teachers establish what learners already know and how much experience and exposure they have had online through targeted questioning.
- As well as forming an integral part of the computing curriculum, online safety is taught in the context of PSHCE and RSE.
- Whenever ICT is used throughout the curriculum, our online safety rules are discussed and referred to.

How do we manage social networking technologies?

It is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism of social networking and blogging sites. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, Redhill and Thomas Telford Primary endeavours to deny access to social networking sites to students within school: this includes access to sites like Facebook.
- All students are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the

appropriateness of any images they post due to the difficulty of removing an image once online.

- Students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, School details, IM/ email address, specific hobbies/ interests).
- Our older students, and their parents, are reminded that they are not old enough to hold an account on many social media sites including 'Facebook' although are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals when they are old enough.
- Students are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our students are asked to report any incidents of bullying to the school immediately.
- Staff may only create blogs, wikis or other spaces in order to communicate with students using the LA Learning Platform or other systems approved by the Head teacher, for example, Purple Mash.
- Members of staff are prohibited from having any communication to students via social networking sites.
- Any repeated attempts by students to contact staff must be reported to the Head.

How do we manage AI?

The schools recognise the increasing use of generative AI technologies by children and adults.

Online safety education will include:

- safe and responsible use of AI tools;
- identifying misinformation and disinformation;
- recognising AI-generated content;
- understanding the risks associated with AI chatbots;
- protecting personal information when using AI tools;
- awareness of AI-generated harmful, abusive or inappropriate content.

The schools will treat AI-generated harmful content, including manipulated images and deepfakes, as safeguarding concerns where appropriate.

Please see our Safe Use of Artificial Intelligence (AI) Policy and our AI Privacy Notice for further information.

How do we manage online safety incidents?

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the online safety co-ordinator, computing co-ordinator or other member of the Senior Leadership Team. Where a child has accessed extremist materials online and may be susceptible to

radicalisation, the DSL in conjunction with the Prevent lead, will contact the local authority and/or police following the Prevent pathway, which may lead to making a referral to the Channel programme. Where a child has been subject to cyber-bullying, we will follow procedures set out in our child-on-child abuse policy in consultation with our relationships and behaviour policy.

- For inappropriate use or misuse by a pupil, the event will be recorded on CPOMS and tagged as an 'ESafety' incident.
- The online safety coordinator is able to view and monitors all incidents on CPOMS tagged as 'ESafety' incidents.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the online safety co-ordinator, depending on the seriousness of the offence; investigation by the Head teacher/ LA/ social services/police might lead to immediate suspension, possibly leading to exclusion (student) dismissal and involvement of police for very serious offences (staff)

Useful resources for staff

Childnet – Provides guidance for schools on cyberbullying

Educateagainsthate – Provides practical advice and support on protecting children from extremism and radicalisation

London Grid for Learning – Provides advice on all aspects of a school or college's online safety arrangements

NSPCC E-safety for schools – Provides advice, templates, and tools on all aspects of a school or college's online safety arrangements

Safer recruitment consortium – 'Guidance for safe working practice', which may help ensure staff behaviour policies are robust and effective

Searching screening and confiscation – Departmental advice for schools on searching children and confiscating items such as mobile phones

South West Grid for Learning – Provides advice on all aspects of a school or college's online safety arrangements

Use of social media for online radicalisation – A briefing note for schools on how social media is used to encourage travel to Syria and Iraq

Online Safety Audit Tool – From UK Council for Internet Safety to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring

UK Safer Internet Centre – Provides tips, advice, guides and other resources to help keep children safe online

Useful resources for children

Childline – For free and confidential advice

UK Safer Internet Centre – To report and remove harmful online content

CEOP Safety Centre – to report online child sexual abuse

Useful resources for children

Childnet – Offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support

Commonsensemedia – Provides independent reviews, age ratings, & other information about all types of media for children and their parents

Government advice – About protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

Internet Matters – Provides age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world

How Can I Help My Child? – Marie Collins Foundation – Sexual abuse online

London Grid for Learning – Provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

Stopitnow resource from The Lucy Faithfull Foundation – Can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

CEOP Education – Provides information, guidance and resources for support for parents and carers, helping them to protect their child(ren) from online sexual abuse

Parentzone – Provides help for parents and carers on how to keep their children safe online

Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parental guide on talking to their children about online sexual harassment