Redhill Primary Academy

Online Safety Policy

Signed

Ms Fiona Seddon

Chair of Governors

September 2023

Redhill Primary Academy
Online Safety Policy

At Redhill Primary Academy, 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 school 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 school provides a broad and balanced online safety curriculum;
- To ensure that the school has 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 school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named online safety coordinator in our school is **Amy Coughlan**. All members of the school community have been made aware of who holds this post.

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 school’s 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.
- 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.

Other roles and responsibilities

Governors

- 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.

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.

Technical support staff

Technical support staff should ensure the following:

- The school's ICT infrastructure is secure and is not open to misuse or malicious attack.
- Users may only access the school's 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:

- They have an up-to-date awareness of online safety matters and of the current school online safety policy and practices.
- They have read, understood and signed the school 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 school 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 school's 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 school's 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 should ensure the following:

- Use the school ICT systems in accordance with the age-specific Pupil Acceptable Use Policies, which they or their parents 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 school's 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 school website and the school 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 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 school 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 Redhill website).

What dangers could children face online?

Technology offers unimaginable opportunities and is constantly evolving. Access is currently becoming universal and increasingly more mobile, and pupils are using technology at an ever earlier age. The use of these new technologies can put young people at risk within and outside the school. Some of the dangers they could face are listed below:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to / loss of / sharing of personal information;
- The risk of being subject to grooming by those with whom they make contact on the internet;
- The sharing / distribution of personal images without an individual's consent or knowledge;
- Inappropriate communication / contact with others, including strangers;
- Cyber-bullying;
- Access to unsuitable video / internet games;
- An inability to evaluate the quality, accuracy and relevance of information on the internet;
- Illegal downloading of music or video files;
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

The breadth of issues classified within online safety is considerable, but can be categorised into four main areas of risk.

	Content Child as recipient	Contact Child as participant	Conduct Child as actor	Contract Child as consumer
Aggressive	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
Sexual	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
Values	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
Cross-cutting	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

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

Content	All staff use Videolink when sharing YouTube videos to prevent children being exposed to inappropriate advertising. 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?***
Contract	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?

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 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 by the online safety co-ordinator and a DSL if required. 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 type 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.
- 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 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 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.

- For inappropriate use or misuse by a pupil, the event will be logged in the online safety log, located in the head teacher's office and will also 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 websites

https://www.thinkuknow.co.uk/	NCA CEOPs advice on online safety
https://www.disrespectnobody.co.uk/relationship-abuse/what-is-relationship-abuse/	Home Office advice on healthy relationships, including sexting and pornography
https://www.saferinternet.org.uk/	Contains a specialist helpline for UK schools and colleges
https://www.internetmatters.org/?gclid=EAIaIQobChMIktuA5LWK2wIVRYXVCh2afg2aEAAYASAAEgIJ5vD_BwE	Help for parents on how to keep their child safe online
https://parentzone.org.uk/be-internet-legends	Help for parents on how to keep their child safe online
https://www.childnet.com/resources/cyberbullying-guidance-for-schools	Guidance for schools on Cyberbullying
https://www.pshe-association.org.uk/	Guidance and useful teaching resources covering inline safety issues including pornography and the sharing of sexual images
https://www.gov.uk/government/organisations/uk-council-for-internet-safety	The UK council for internet safety's website provides sexting advice, online safety, education for a connected world framework
https://www.net-aware.org.uk/	NCPCC advice for parents
https://www.commonsensemedia.org/	Independent reviews, age ratings & other information about all types of media for children and their parents
https://educateagainsthate.com/	Provides practical advice and support on protecting children from extremism and radicalisation
https://www.lgfl.net/online-safety/default.aspx	Provides practical advice and support on protecting children from extremism and radicalisation
https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools	Provides advice on all aspects of a school or college's online safety arrangements
https://www.saferrecruitmentconsortium.org/	"Guidance for safe working practice", which may help

	ensure staff behaviour policies are robust and effective
https://www.gov.uk/government/publications/searching-screening-and-confiscation	Departmental advice for schools on searching children and confiscating items such as mobile phones
https://swgfl.org.uk/	Provides advice on all aspects of a school or college's online safety arrangements
https://www.gov.uk/government/publications/the-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
https://www.gov.uk/government/publications/ukcis-online-safety-audit-tool	UK Council for Internet Safety have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring