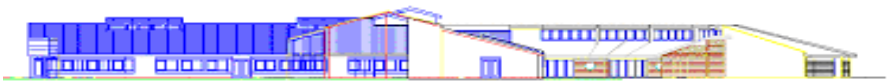
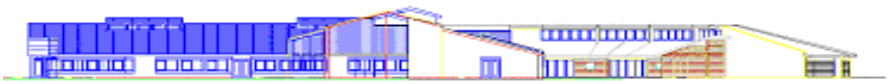


Redhill Primary School

E safety/awareness Policy

Signed

Mrs Beth Tutchener-Ellis, Chair of Governors



Aims

- to protect and educate pupils and staff in their use of technology
- to have the appropriate mechanisms to intervene and support any incident where appropriate.
- to ensure pupils are fully aware of different forms of bullying including cyber bullying and actively try to prevent it from occurring
- to promote a culture of safety, including e safety

It is our responsibility

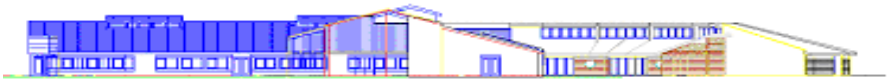
- To protect and educate pupils and staff in their use of technology
- To have appropriate mechanisms to intervene and support any incident where appropriate

In light of the above aims, at Redhill we will;

- audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school
- use pupils' and families' views more often to develop e-safety strategies
- manage the transition from locked down systems to more managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school
- provide an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies
- work with their partners and other providers to ensure that pupils who receive part of their education away from school are e-safe
- systematically review and develop their e-safety procedures, including training, to ensure that they have a positive impact on pupils' knowledge and understanding

The computing curriculum now consists of three main aspects. These are **Digital literacy, Computer studies** and **Information technology**. The internet will play a large part in all three aspects. At Redhill 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 E-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 e-safety policy helps to ensure safe and appropriate use.



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 may face include

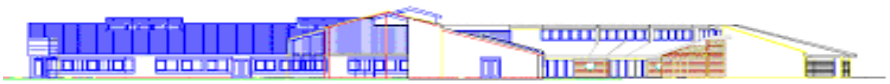
- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's 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 internet can be accessed from many devices from smartphones to tablets, computer and games consoles. The internet provides a lot of opportunities for interaction with other people, not only by leaving messages on social media sites or sending emails, but also by direct interaction for example in a lot of games and video streaming services. These services can include both voice or and video transmission.

Some of these risks reflect situations in the real world also and so this policy is used in conjunction with other school policies. (Behaviour, anti-bullying and child protection.) As with all risks it is impossible to eliminate them completely therefore the school has put into place measures to ensure we have done everything that could reasonably be expected of us to manage and reduce these risks.

The risks:

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	advertisements spam sponsorship personal information	violent/hateful content lifestyle sites	pornographic or unwelcome sexual content	bias racist misleading information or advice
Contact (child as participant)	tracking harvesting personal information	being bullied, harassed or stalked	meeting strangers being groomed	self-harm unwelcome persuasions
Conduct (child as actor)	illegal downloading hacking gambling financial scams terrorism	bullying or harassing another	creating and uploading inappropriate material; sexting	providing misleading info and advice health and wellbeing; time spent online



After carrying out a questionnaire the E-awareness committee found out that of the children we asked;

- 44% of the children use the internet every day and 38% use it more than once a week.
- 28% of children have played an online game with someone they have never met.

For this reason we feel the children need to be aware of the three main risks whilst online.

We update staff and students (as appropriate based on age) of developments in the three areas of risk

1. Content

Exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse	School uses kids rex as a search engine and higher up in school children are taught how to use Google safely. Teachers ensure preferences in settings are suitable. When searching for images on the internet the children use safe search engines although if something inappropriate does appear they know to close it and report it to an adult.
Lifestyle websites, for example pro - anorexia/self-harm/suicide sites	All internet activity is monitored and inappropriate use or searches for issues as detailed on the left are captured by Policy Central.
Hate sites	
Content validation: how to check authenticity and accuracy of online content	

2. Contact

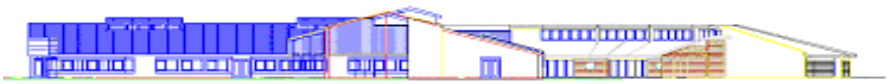
- Grooming
- cyber - bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

3. Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well - being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self generated indecent images)

Whole school consistent approach:

- All teaching and non-teaching staff can recognise and are aware of e-safety issues.
- High quality leadership and management make e-safety a priority across all areas of the school.



- A high priority is given to training in e-safety, extending expertise widely and building internal capacity.
- The contribution of pupils, parents and the wider school community is valued and integrated.

Managing 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 on the Schools-Guest wireless system via their own laptops or mobile devices.
- 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 are reminded that they are not old enough for a 'Facebook' account 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
- 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 teacher.

Roles and responsibilities

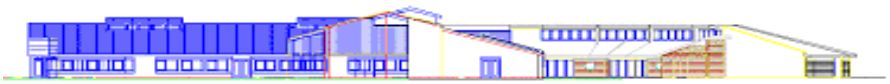
The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports.

Headteacher and Senior Leaders

- The Headteacher is responsible for ensuring the safety (including e-safety) of 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 e-safety allegation being made against a member of staff.



E – Safety Co-ordinator

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with T and W ICT technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- liases regularly with ICT link governor to discuss current issues, review incident logs and filtering / change control logs

Technical staff

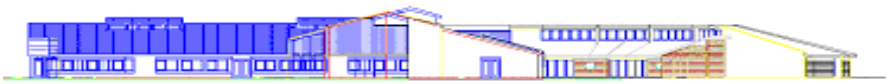
The Local Authority and ICT Technician are responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- that he / she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that 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 E-Safety Co-ordinator
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the E-Safety Co-ordinator or other member of the Senior Leadership Team
- digital communications with students / pupils (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- pupils understand and follow the school e-safety and acceptable use policy
- they monitor ICT activity in lessons, extra curricular and extended school activities



- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be 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.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the School community
- All staff are encouraged to incorporate eSafety activities and awareness within their curriculum areas

E-safety Incident Log -

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Head teacher and Computing coordinator.
- For inappropriate use or misuse by a student the event will be logged in the e-safety log, located in the head teacher's office.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety 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)

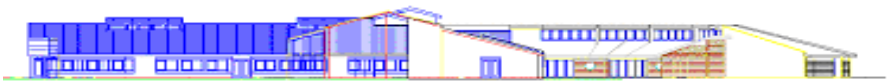
<u>Designated person for child protection / Child Protection Officer</u>

Should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

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

<u>Pupils</u>

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Policy, which they and/or their parents will be expected to sign before being given access to school systems.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to 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.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-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 e-safety coordinator or teacher as appropriate

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. The school will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website / VLE and information about national / local e-safety campaigns / literature.

Parents and carers will be responsible for:

- endorsing (by signature) the Student / Pupil Acceptable Use Policy
- accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy.

We believe that it is essential for parents / carers to be fully involved with promoting eSafety both in and outside of Redhill and also to be aware of their responsibilities. We regularly consult and discuss eSafety with parents / carers and seek to promote a wide understanding of the benefits related to ICT and associated risks

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to Redhill
- 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)
- Redhill disseminates information to parents relating to eSafety where appropriate in the form of:
    - Information and celebration evenings
    - Posters
    - Website/ Learning Platform postings
    - Newsletter items

Users are made aware of sanctions relating to the misuse or misconduct by the Class teacher and Head teacher.