Warlingham Park School
E-Safety Policy

This policy applies to the whole school, including the EYFS

1. Introduction

E-Safety encompasses the use of Internet technologies and electronic communications, such as mobile phones, as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

The school's e-safety policy should operate in conjunction with other policies including those for Behaviour and Discipline, Anti-bullying, Curriculum, Safeguarding and Data Protection.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband, including the effective management of filtering systems

2. School e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies, including child protection.

The Headteacher and Deputy Head work in close co-operation to implement this policy and are Designated Child Protection Officers. References to e-safety issues are included in the Child Protection, Health and Safety, and Anti-Bullying policies.

Our e-Safety Policy has been written by the school. It has been agreed by the staff and governors. (The appendix shows the set of rules, developed by the pupils, which apply to pupil use of the ICT Suite.)

3. Roles and Responsibilities

All staff are responsible for ensuring that they use the school computers responsibly and do not personally access inappropriate content on the internet whilst at school. Detailed guidance is provided in the Staff Handbook, Code of Conduct and Acceptable Use guidelines.

The Head has ultimate responsibility for e-safety issues within the school including:

- Implementation of the school's e-safety policy
- Ensuring that e-safety issues are given high profile
- Linking with Trustees, parents and staff to promote e-safety
- Ensuring e-safety is embedded in the curriculum
- Ensuring that all reasonable precautions are taken to ensure that pupils cannot access inappropriate materials
- Deciding on sanctions against staff and pupils in breach of policies
- Ensuring that all staff have received e-Safety training

Any e-safety issues which may have serious implications for a child's safety or their wellbeing should be referred to one the DSLs without delay. Advice will be sought from the Surrey Safeguarding Children Board if escalation may be required.

4. Working with Parents

Parents are expected to support the school's e-safety strategies and policies, and should talk to their children about the Internet Rules in Appendix A.

Parents should not give their child a teacher's school email address. Any electronic communication should be made between the parent and the teacher.

Information about e-safety will be shared with parents periodically and in a variety of different forms, eg. 'Internet Safety' booklet and 'Digital Safety' articles on the website and workshops held every few years.

The website www.internetmatters.org helps parents to keep their children safe online. DfE advice about cyberbullying can be accessed by clicking the following link for parents.

5. Teaching and learning

Internet use is important. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning. The school's Internet access is designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use through their ICT lessons.

Internet access will be planned to enrich and extend learning activities. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

One of the key features of our e-safety strategy is teaching pupils to protect themselves and behave responsibly while online. The Headteacher has overall responsibility for the coordination of e-safety education, but all teaching staff play a role in delivering e-safety messages in language which is appropriate to their age.

Pupils are taught:

- The benefits and risks of using the internet
- How their behaviour can put themselves and others at risk
- How adjusting their behaviour can reduce risks and build resilience, including to radicalisation
- What strategies they can use to keep themselves safe
- About the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults
- What to do if concerned about something they have seen on the internet
- Who to contact with concerns
- That the school has a 'no blame' policy so pupils are encouraged to report any e-safety incidents
- The school has a 'no tolerance' policy regarding cyberbullying
- That behaviour that breaches acceptable use will be subject to sanctions and disciplinary action

In the event that a pupil accidentally accesses inappropriate materials they must report this to an adult immediately and take appropriate action to hide the screen or close the window so that an adult can take the appropriate action. Where a pupil feels unable to disclose abuse or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk or ceop.police.uk) to make a report or seek further advice.

Delivering e-safety messages

- Teachers are responsible for delivering an on-going e-safety education in the classroom and will undertake regular training (normally annually) to ensure that they are up-to-date with current practice.
- Reminders are given to pupils by teachers at the start of each academic year and in specific lessons regarding the acceptable use of the internet and how to keep safe.
- Appropriate supervision is provided to ensure that pupils are accessing suitable age appropriate sites, and staff remain vigilant when computers are being used.
- Rules regarding safe internet use are clearly displayed in various relevant places.
- Pupils are expected to follow the Computer Suite Rules. Teachers refer pupils to these at the start of each academic year.

The following aspects of online education will be covered at various points in the curriculum:

Self-image and Identity; Online relationships; Online reputation; Online bullying; Managing online information; Health, wellbeing and lifestyle; Privacy and security; Copyright and ownership.

Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Deputy Head.
- Staff should ensure that the use of Internet-derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Pupils with special needs

Pupils with learning difficulties and/or any disabilities may be more vulnerable to risk from use of the internet and will require additional guidance on e-safety practice as well as closer supervision. The SENCO ensures that the school's e-safety policy is adapted to suit the needs of pupils with special needs. They liaise with parents and other relevant agencies in developing e-safety practices for pupils with special needs and to keep up to date with any developments regarding emerging technologies and e-safety and how these impact on pupils with special needs.

6. Managing Internet Access

Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses broadband with its firewall and filters.

Pupils may only use approved e-mail accounts on the school system and are not allowed access to personal e-mail accounts or chat rooms whilst in school. Pupils must immediately tell a teacher if they receive offensive e-mail.

Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.

Any published content on the contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.

The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.

Pupils' full names will not be used anywhere on the Website, particularly in association with photographs.

Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing
Social networking sites and newsgroups will be blocked unless a specific use is approved. Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs, etc.

Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.

Managing filtering
The school will work in partnership with the service provider to ensure filtering systems are as effective as possible. If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.

Staff should ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Protecting personal data
Personal data will be recorded, processed, transferred and made available according to the GDPR regulations.

7. Policy Decisions

Authorising Internet access
The school will maintain a current record of all staff and pupils who are granted Internet access.

At FS/Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Assessing risks
In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

The Headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

Handling e-safety complaints
Complaints of Internet misuse will be dealt with by either the Headteacher or the Deputy Head. Any complaint about staff misuse must be referred to the Headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Pupils and parents will be informed of the complaints procedure.
Sanctions within the school discipline policy include:
– interview/counselling by class teacher / Headteacher;
– informing parents or carers;
– removal of Internet or computer access for a period

Community use of the Internet
The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

8. Communications Policy

Introducing the e-safety policy to pupils

- Rules for Internet access will be posted in the ICT Suite.
- Pupils will be informed that Internet use will be monitored.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.

Staff and the e-Safety policy
All staff will be given the School e-Safety Policy and its importance explained.
Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' / carers' support
Parents' / carers' attention will be drawn to the School e-Safety Policy in newsletters.

9. Cyberbullying

Cyberbullying is the use of electronic technology, repeated over time, to intentionally hurt or upset someone. This includes devices and equipment such as computers, tablets and phones as well as communication tools including social media sites, text messages, chat and websites. The internet allows bullying to continue past school hours and invades the victim's home life and personal space and allows for hurtful comments and material to be available to a wider audience.

Examples of cyberbullying include:

- Rude, abusive or threatening messages via e-mail, text, gaming or social networking sites.
- Posting insulting, derogatory or defamatory statements or spreading rumours on blogs or social networking sites.
- Setting up websites that specifically target a victim.
- Making or sharing derogatory or embarrassing photos or videos of someone via

mobile phone or e-mail.

- Being purposely excluded from a group eg. Whats App.

Cyberbullying can affect both pupils and staff and it could be deemed a criminal offence. Incidents of cyberbullying will be reported to the Headteacher or Deputy Head and, if extreme, may in turn be reported to the police. Pupils are taught to only give out mobile phone numbers and e-mail addresses to trusted people; not to respond to offensive messages and to report these immediately to an appropriate adult.

Website providers and mobile phone companies are aware of the issue of cyberbullying and have their own systems in place to deal with problems, such as tracing and blocking communications and will give advice to parents and teachers on request.

10. Monitoring and Review

This policy will be formally reviewed every two years, however it will be amended earlier if legislation or school procedures change prior to that time. The Headteacher will monitor this policy's effectiveness.

Revised: September 2018

This policy will be reviewed every 2 years	
Title	e-Safety
Author	Sarah Buist (Headteacher)
Approved by SMT	02.09.2018
Approval/Review required by Trustees	Yes 04.09.2018
Latest Review (were changes made)	Yes, September 2018
Next Review Date	September 2020

Appendix

ICT suite and internet pupil rules

Our Computer Suite and Internet rules.

- We will only use the internet with a member of staff present.
- We will only visit websites that have been approved by a member of staff.
- We will only use the computers and the internet for schoolwork.
- We will not bring memory sticks into school because these might introduce viruses to the school system.
- We will only e-mail people my teacher has approved.
- We will always give my e-mail a subject.
- We will not open any e-mail or attachment if I don't know who has sent it to me or it has no subject.
- The messages I send will be polite and sensible.
- We will not give my home address or phone number or arrange to meet someone over the internet or by e-mail.
- To help protect other pupils and myself, I will tell a teacher if I see anything on the Internet that I am unhappy with or if I receive messages I do not like.
- We understand that the school will check the Internet sites I visit.
- We will treat our computers and the computer suite with care.