Orley Farm School

E-Safety Policy

(Whole School Including EYFS)

First Issued:	February 2011	**Next Review:**	Summer Term 2020
Reviewed:	Summer Term 2019	**Version:**	2.0
Responsible:	Director of Finance and Operations (DFO) and Deputy Head (Academic)		

1. Aims

a. In support of Orley Farm School's (the School) Safeguarding and Curriculum Policies the aim of this policy is to make clear the school's approach to E-Safety. It makes clear what good practice is and gives guidance as to how to support pupils in the use of Internet technologies, electronic communications and their ability to safely access Internet information. It sets out the steps staff should take to take care of their own safety and security. It also aims to educate parents and make them aware of the risks children face at home.

2. Objectives

a. To ensure pupils and staff are aware of the issues surrounding E-Safety. This encompasses Internet technologies, social networking and electronic communications such as mobile phones and wireless technology.

3. World Wide Web

a. A sophisticated filtering system is in place to ensure children's safety. Searches of the Internet are only permitted when a member of staff is supervising the session. If staff or pupils discover unsuitable sites, the URL (address), time and content must be reported to the IT Manager.

b. Pupils can only use approved e-mail accounts on the School system. These accounts are monitored by child protection software and email filtering systems.

c. Pupils are taught and encouraged to tell a trusted adult immediately if they receive offensive e-mail (either within school or at home) or if they become aware of any attempts by people who they don't know trying to contact them.

d. Pupils are taught never to give out personal details of any kind, including their email address, in a public setting (virtual or real) or divulge personal details which may identify them or their location.

e. Use of traditional social networking sites, newsgroups or forums/chat rooms in School is not permitted. However, use is made of educationally based websites that permit file sharing and pupil interaction. These websites are moderated and used subject to adult supervision. The School informs parents if their child is to use such a website as part of the curriculum.

f. Pupils are advised not to place personal photos on any website.

4. Mobile Phones

a. Children are not permitted to use mobile phones whilst on the School site, during school hours or whilst participating in school activities. In exceptional circumstances, when pupils in Years 7 and 8 are permitted by parents to travel to and from school independently, mobile phones may be kept during the day in the School Office.

5. Publishing content and the School website

a. The contact details on the school website are the school address, e-mail and telephone number. Staff and pupils' personal contact information is not published.

b. The School maintains a current record of how and where pupils' photographs and work may be published. Parents are asked to update the Use of Images Consent Form annually.

c. Photographs that include pupils are selected carefully, subject to parental consent and are appropriate for the context.

d. Pupils' full names are not published anywhere on promotional material or solid media in association with photographs.

6. Information System Security

a. Virus protection has been installed and is updated regularly by the Network Manager through anti-virus software.

b. Security strategies are discussed by the Senior Leadership Team, Network Manager and other relevant staff. The Network Manager then updates and implements changes to the system.

c. The School's wireless network is encrypted to prevent unauthorised access.

7. Child Protection

Guidelines on Cyberbullying

a. As part of our mandatory anti-bullying policy the school has child protection software. This supports, where applicable, our ability to:

1. Apply a policy to monitor electronic messages and images;
2. Monitor all e-communications used on the school site through our filtering system;
3. Work with pupils to make sure new communication technologies are used safely;
4. Teach children safe Internet behaviour;
5. Alert staff to potentially dangerous incidents, such as self-harm, abuse or attempts at predator grooming. Through the use of child protection software evidence is captured to provide appropriate help to a child who is at risk.

8. Using the Internet in School

a. The use of the internet at the School is for educational purposes only.

b. The Internet access at school for pupils has been designed expressly to include filtering appropriate to the age of the pupils.

c. Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Rules for Internet access are posted in all Computer Suites. Internet safety forms discussions, at an appropriate level for Pre Prep, and they are reminded about safe computer use in lessons. The rules for Internet access are in the Pupil Planners for students from Year 3 to 8.

d. All staff have access to the School E-safety Policy. Staff must read the policy at the start of each year and must sign to agree that they will follow procedure.

e. Only users with authorised access are able to use the Internet in school. All staff must read and abide by the 'Acceptable Use of ICT, Phones and Internet' Policy (available on the school network) when considering the use of any Internet and electronic communication based technologies in School.

f. Parents are requested to read the 'Responsible Use of the Internet' and relay this information to their child(ren) joining the school and confirm this via the parent permissions page on Firefly.

g. The School maintains a current record of all pupils who are granted access to school ICT systems.

h. All pupils have E Safety embedded into the Computer Science curriculum at an age appropriate level.

i. The information in this policy is communicated in simple form to the children from Year 3 via the diary (please see Appendix A).

9. Communication of Policy

a. All parents receive a copy of Digital Parenting and links to appropriate websites are available on our own website. Information Evenings are held to educate parents and carers and we optimise all opportunities for disseminating updates at relevant events throughout the year.

b. Protecting Personal Data

In accordance with the Data Protection Act 2018, users are not allowed to access other users' personal files and folders, including School e-mail. The exception to this being the ICT Network Manager who can gain access through permission from the Director of Finance and Operations and Information Officer (in their capacity as data controller) when just cause has been established.

10. Assessing Risk

a. Filtering of the School's Internet content is provided by web content filtering software. This software filters the actual content of pages based on many methods including phrase matching, PICS filtering and URL filtering.

b. Every effort is taken to block inappropriate content in all situations however, there is no fail-safe way and therefore the School cannot take responsibility for these events when all reasonable steps have been taken.

11. Handling e-safety complaints

a. Complaints of Internet misuse at school or within school remit are dealt with by the Head of Computing and a Deputy Head.

b. Any complaint about staff misuse must be referred to a Deputy Head.

c. Complaints of a child protection nature must be dealt with in accordance with the School child protection procedures. Please refer to the school's Safeguarding & Child Protection Policy (available on the school website).

12. Monitoring and Evaluation

a. The members of the Curriculum Team together with the Headmaster monitor and evaluate this policy.

Appendix A

E-Safety Page

It is very important that you feel safe when using the internet and your e-mail account at school. Here are some tips that might help you.

- Never hand out any personal information when using the Internet. Things such as your full name, passwords, e-mail address, home address, telephone number or even a photograph of yourself, should always be kept secret.
- Don't open any emails from people that you don't know. They could contain viruses or nasty messages. Press delete.
- Never respond to any kind of online communication from people you don't know. Not everyone online is who they say they are.
- Not everything you read on the Internet is true. Check your sources carefully.
- Never arrange to meet with any stranger who contacts you online.
- Never use e-mail or the Internet as a way to bully people or send them horrible messages.
- You are responsible for everything you write in an email or online and everything written in school is monitored. If in doubt DON'T!
- Close down any webpage you come across that contains anything unpleasant or inappropriate, and report it to your teacher straight away.
- FINALLY, if there is anything that makes you feel unhappy, uncomfortable or worried whilst you are using e-mail or the Internet in school, you must make sure you contact any teacher or adult who works in the school. Even if you think it is something trivial, it is still important to let us know.