Ocklynge Junior School E-Safety Policy

This policy should be read in conjunction with the schools Computing Policy, Social Media Policy, Staff AUP and 'Internet Golden Rules'.

Background

The internet has been a part of modern life for the last 20 years and the school and the school sees it as a valuable resource to both pupils and teachers for teaching and learning. Users have access to thousands of libraries and databases. Electronic information research skills are now fundamental to preparation for living and working in society. The school will integrate such information and skills as appropriate within the curriculum and staff will provide guidance and instruction to pupils in the appropriate use of such resources. As with any system as large as the internet there are risks, but the advantages of working in a connected world, far outweigh them. At Ocklynge we take e-safety seriously and review our practices and procedures annually.

Communication

The means of communication have expanded rapidly since the turn of the millennium and will continue to do so. We provide an environment where pupils and staff can communicate with a range of audience, from emailing people across the room to skyping or blogging our link schools around the world. Pupils are provided with their own email address which is provided and monitored by the school. In their first term at Ocklynge they are taught about the safe use of email, and this is continued throughout the school as issues are flagged up by the monitoring systems in place.

All communication that takes place between staff and outside agencies must take place through the school email system or the county provided secure mail system.

Each year group has a link with a school in another country and ICT can greatly enhance the benefit that children get from this link. As a school we want to be able to use new methods of communicating with them while maintaining appropriate safeguards.

Internet safety

It is acknowledged that there are inappropriate and offensive materials on the internet. There are also people who seek to abuse the internet. To avoid pupils accessing such sites, they will not be given access to the Internet without teacher supervision. In addition the school uses its own filtering software in tandem with Research Machines filtering which blocks out most web pages containing unsuitable content. In the event of inappropriate material not being screened out, the school will take proactive measures to inform parents and RM/SEGFL so that the website concerned is blocked. The school monitors all internet activities accessed by pupils and staff.

Children are taught e-safety based on the East Sussex School Improvement Service scheme of work but with additional material to ensure that developing issues are covered fully. We expect children to exercise a growing awareness and use of safe practices.

If there is an incident of deliberate inappropriate use of school equipment, the evidence trail will be preserved. Two people will bag up the workstation and sign for it. The E-Safety officer (the Headteacher) is then responsible for taking appropriate action. Ocklynge School has also introduced another layer of filtering for web and email content, so essentially a two tier approach of firewall/web/email content filtering takes place.

Internet Use Guidelines

To ensure that pupils benefit from the school's Internet resources, all pupils are expected to adhere to the guidelines in 'The Internet Golden Rules' document.

Pupil's Acceptable Use Policy

During the first week of the new academic year the pupils are required to understand and sign the class Internet Golden Rules.

Procedures for dealing with breaches of the Acceptable Use Policy

If a pupil is found to have been trying to access unsuitable sites, sending threatening or offensive e-mails, or breaking any other of the Acceptable Use Policy guidelines, appropriate action will be taken. The incident will also be dealt with in accordance with the school discipline policy. The same procedures will apply to message posted on blogs or forums. Cyber bullying, (using the internet to intimidate, threaten or bully others) is totally unacceptable. The school makes no distinction between where or when such events occur. If it happens, we want to know about it and will deal with it accordingly. Parents or pupils who encounter e-safety issues, are encouraged to use the normal channels of communication to bring these to the attention of the school.

If any member of staff encounters a breach of the e-safety policy, they must fill in an incident form, isolate any machines involved, and inform the Headteacher or SENCO.

School Intranet

Staff have a unique, strong password that is needed to access the School's Network. These passwords are changed regularly. Pupils also have a password that allows them access to the Public drive, and their own drive. Remote access to the School Network is made possible through the use of a Citrix server. This also is password protected.

Staff AUP

Staff are provided with access to the Internet at school, but must first sign the Acceptable Use Statement for Staff.

School Web Site

Children's work will only be identified by first names. Photographs of children will not be accompanied by names. Parents are informed of this via the school Information handbook, and they may contact the school if they would rather their child's photograph was not used.

November 2015

E-Safety Working Group

(Headteacher, ICT co-ordinator, Network Manager).