
On-Line Safety

Ardleigh Green
Junior School

September 2017



Introduction

The On- Line Safety Policy relates to other policies, including those for ICT, Bullying and Child Protection. The roles of the co-ordinator will overlap with those of the ICT and designated Child Protection Co-ordinator.

Teaching and Learning

Ardleigh Green believes that the Internet is an essential part of 21st century living and plays an important part in education, business and social interaction. Our 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 both staff and pupils.

Internet Use

- The school Internet access is specially designed for pupil use and includes filtering appropriate to the age of our pupils.
- Pupils will be taught what acceptable Internet use is and what is not through clear objectives during lessons.
- Pupils will be educated in effective use of Internet research, including; retrieval of information and reliability of information found and the need to cross-check information for its accuracy.
- Pupils will be taught how to present and publish work to a wider audience using the Internet.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught how to report unpleasant Internet content.

Managing Internet Access

System Security & Filtering

- School ICT systems of security are reviewed regularly.
- Virus protection is updated on a regular basis.
- The school works with the LA and LGfL to ensure systems to protect pupils are reviewed and improved.
- If staff find unsuitable online materials the site must be reported to the ICT subject leader, who will ensure that the site is filtered out in future.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils are taught to tell an adult immediately if they receive an offensive e-mail.
- In e-mail communication pupils are taught not to reveal personal details or arrange to meet anyone.
- Incoming e-mails should be treated as suspicious and attachments not opened unless the author is known.



Published Content – School Website

- Staff or pupil personal information will not be published. The contact details given online is that of the school office.
- The Head Teacher, along with the ICT subject leader will ensure content is accurate and appropriate.

Publishing Pupils Images

- Photographs that include pupils will be selected carefully so that it is difficult to identify individual children.
- Written permission is sought from parents/guardians before photographs are published.
- Pupils' full names will not be used online nor accompany pupils' images.
- Any pupils' work published online will show only their Christian names.
- Parents are informed of the school's policy when their child first enters the school.

Social Networking

- The school has blocked access to social networking websites (Facebook etc), although pupils are informed of how to stay safe if using such a website. The school uses Twitter to communicate with parents and there is a Twitter feed on the school website. The content contained on the school's Twitter account is monitored by the headteacher and Leader for Computing
- Pupils are advised never to give out personal details of any kind which may identify them, their friends or family.

Managing Video Conference and Webcam Use

- All video conferencing uses the school's broadband network to ensure quality of service and security.
- When making a video conferencing call the school will ensure that an adult is present at all times.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and any risks will be considered before use is allowed in school.
- Currently mobile phones are not allowed in school, as the mobile Internet element can bypass school filtering systems. There is a detailed mobile phone policy in relation to staff use.



Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

School Policies

- All staff must read and sign the 'Acceptable Use' Policy
- The school maintains a current record of all staff and pupils who are granted access to school ICT systems.
- It is the responsibility of the class Teacher to assess whether the Internet material being looked at is appropriate to the task.
- Parents are also asked to sign and return an Internet Permission Form.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material on the Internet. However, due to the scale and ever changing nature of the Internet, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school system.
- The school will audit ICT use to establish if the On-Line Safety policy is adequate, appropriate and effective.

On-Line Safety Complaints

- Complaints of Internet misuse will be dealt with by the Head Teacher.
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding and child protection procedures.
- Pupils and parents are informed of consequences for pupils misusing the Internet.

On-Line Safety Staff and Pupils

- Pupils are taught about E-Safety at the beginning of each Computing Lesson. This is reinforced through assemblies and PSHE and our weekly on-line safety training undertaken annually by staff and pupils. The school also holds an annual On Line Safety Training session for parents which is led by the Local Authority.
- E-Safety posters are on display in the ICT suite and throughout the school.
- Pupils are aware that computer and Internet use can be monitored and, if needed, will be followed-up appropriately
- On-Line Safety is embedded within the Computing scheme of Work.
- All staff are given the On-Line Safety Policy and its importance explained.

