Castle Hill St Philip's CE Primary

E-SAFETY POLICY

RATIONALE

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

The e-safety policy will operate in conjunction with other polices including those for Computing, Behaviour, Bullying, Curriculum, Data Protection and Security.

AIMS

The aim of the e-safety policy is to ensure:

- Responsible 'Computing' use by all the staff and children
- Secure school network design and use
- Safe and secure broadband access

TEACHING AND LEARNING

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 high-quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary learning tool for staff and pupils.

The school Internet access will be designed expressly for the use by children and will include filtering appropriate to the age of the pupil.

Children will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. These rules will be displayed in every classroom. They are discussed periodically in each cohort (See Appendix 1).

MANAGING INTERNET ACCESS

a) Information system security

- Schools Computing systems capacity and security will be reviewed regularly
- Virus protection (Sophos Anti-Virus) will be updated regularly
- Impero Software will be employed to monitor appropriate use of Computing resources by children and adults.

b) Published content and the school website

- Staff or pupil personal contact information will not be published. The contact details given online are the school office.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

c) Publishing pupil's images and work

- Pupils' full names will be not be used anywhere on the web site- particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site.
- Pupils' work can only be published with permission of the pupil and parents.

d) Social networking and personal publishing

- Access to other social networking sites, other than The Bridge, is not permitted and will be blocked/ filtered. Impero Software will alert the E-safety leader- if this rule is breached.
- The school will educate children in the safe use of social networking sites, through our digital citizens element of the computing curriculum and our annual E-Safety day.
- Children and parents will be advised that the use of social network sites like Facebook and Twitter are inappropriate for primary aged children.
- Children will be advised never to give out personal details of any kind which may identify them or their location.

e) Managing filtering

- The school will work with the LA, DFES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Co-ordinator, who will e-mail the url to filtering@rm.com.

f) Managing videoconferencing

- Videoconferencing will use the educational broadband network rather than the Internet, to ensure quality of service and security.
- Calls will only be made or answered in the presence of a supervising adult.

- Videoconferencing will be appropriately supervised for the children's age.

g) Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The Senior Leadership Team should consider in their policy making that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Where contact with pupils is required to facilitate their learning, staff will be issued with a school phone.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- It should be noted that games machines including the Sony PlayStation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

h) Protecting personal data

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

POLICY DECISIONS

Authorising Internet access

- All staff must read and sign the 'Acceptable Use Policy' before using any school computing resource (See Appendix 2).
- All children and Parents/Carers will be asked to sign an Internet Agreement form in their child's school planner (See Appendix 3).
- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a child's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific approved on-line material.
- In KS2, children will access the Internet with a unique username login so that use of Computing equipment can be monitored at an individual level.

- Access to Wi-Fi and the schools network is password protected. Only users with permission from the Senior Leadership Team will be allowed access.

Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Wigan Council can accept liability for the material accessed, or any consequences resulting from Internet use.

- The school will use e-Safety monitoring software-Impero, and audit Computing use by staff and pupils on a regular basis to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

Handling E-Safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.

- Any complaints about staff misuse must be referred to the head teacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Mobile phones and personal devices

- The use of mobile phones and other personal devices by students and staff in school will be decided by the school and covered in the school Acceptable Use Policy.

- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.

- School staff may confiscate a phone or device if they believe it is being used to contravene the Castle Hill St. Philip's CE Primary School behaviour or bullying policy. The phone or device might be searched by the Senior Leadership Team with the consent of the pupil or parent/carer. If there is suspicion that the material on the mobile may provide evidence relating to a criminal offence the phone will be handed over to the police for further investigation.

- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times in line with school policy.

- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff.

- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor

will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

• Mobile phones and personal devices are not permitted to be used in certain areas within the school site such as changing rooms, toilets and swimming pools.

• Pupils who bring in mobile phones to school should hand them to the teacher or school office for safekeeping until the end of the day.

COMMUNICATIONS POLICY

a) Introducing the E-Safety Policy to Pupils

- E-Safety rules will be displayed in all classrooms and discussed with children at the start of each year.
- Children will be informed that network and Internet use will be monitored.
- Throughout school children are taught how to keep safe online through the digital citizens strand of the Computing curriculum.

b) Staff and the E-Safety Policy

- All staff have access to the School's E-Safety Policy and its importance will be fully explained to all staff.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user using Impero Software. Discretion and professional conduct is essential.

C) Enlisting Parents'/ Carers support

- Parents' attention will be drawn to the school e-safety Policy in newsletters, the school brochure and on the school web site.
- Parents will be informed if children use Computing resources in school in an inappropriate way.
- Parents will be informed if a member of staff becomes aware of an e-safety issue relating to children's use of Computing at home.