

E-SAFETY POLICY

2016-2017

****

**Writing and reviewing the E-safety policy**

The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, anti-bullying and for child safe guarding. The school’s ICT Co-ordinator will also act as E-Safety Coordinator. Our e-Safety Policy has been written by the school, and is in line with government guidance. It has been agreed by senior management and approved by governors. The E-Safety Policy and its implementation will be reviewed annually.

**Teaching and Learning**

**Why Internet use is important**

The Internet is an essential element in the 21st century life for education, business and social interaction. The school has a duty to provide children 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 Internet access is designed expressly for pupil use and includes 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. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

**Pupils will be taught how to evaluate Internet content**

The school will ensure that the use of Internet derived materials by staff and 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.

**Managing Internet Access**

**Information system security**

* School ICT systems capacity and security will be reviewed regularly
* Virus protection is updated regularly
* Advice on security strategies will be monitored on the school’s ICT web page and clarification sought as necessary

**E-mail**

* Pupils may only use approved e-mail accounts on the school system during Computing lessons for subject related purposes
* Pupils email usage should be supervised and monitored by a staff member
* 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
* Adults sending an e-mail to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper
* The forwarding of chain letters is not permitted

**Published content and the school web site**

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 head teacher and ICT co-ordinator 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. Pupils’ full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Pupils’ work can only be published with the permission of the pupil and parents. In the event of an external agency wanting to take and publish pictures of the children, permission should be sought by the agency in the form of a permission slip. Parents will indicate via this slip if they grant permission for such action by the said agency.

**Social networking and personal publishing**

The school will block/filter access to social networking sites. Newsgroups will be blocked. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. It is strongly advised that teachers and staff members at the school should not invite children or active parents to become friends on their social network pages at home as this could lead to issues over their professional conduct which in turn could compromise their role within the school.

**Managing filtering**

* The school will work with the LA, DfE 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 Coordinator
* Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

**Managing video-conferencing**

Video-conferencing will use the educational broadband network rather than the internet to ensure quality of service and security. Pupils will be required to gain permission from the supervising teacher before making or answering a video-conference call. Video-conferencing will be appropriately supervised for the pupils’ age.

**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.

Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

**Protecting personal data**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 e.g. Passwords and information about individuals will be stored securely and can only be released to bodies such as Law enforcement agencies upon correct production of a valid warrant.

**Policy Decisions**

**Authorising Internet access**

* All staff must read and sign the ‘Acceptable ICT Use Agreement’ before using any school ICT resource
* Pupils will be asked to sign a child-friendly version of an ‘Acceptable ICT Use Agreement’
* 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 pupil’s access be withdrawn
* For Early Years/Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials. For Key Stage 2, children will be allowed to use the Internet for research purposes but activity will be carefully monitored by an adult throughout the session

**Assessing risks**

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. Neither the school nor LBWF can accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

**Handling e-safety complaints**

* Complaints of Internet misuse will be dealt with by a senior member of staff
* Any complaint 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
* Pupils and parents will be informed of the complaints procedure
* Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues

**School actions and sanctions**

The school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt using disciplinary procedures for examples, verbal warnings. Staff will need to inform the Headteacher and the Computing Co-ordinator if any incidents such as the ones below are being observed.

**Incidents:**

* Unauthorised use of non-educational sites during lessons
* Unauthorised use of mobile phones and other devices
* Unauthorised use of social media/messaging apps/personal email
* Unauthorised downloading/uploading of files
* Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
* Actions which could bring the school into disrepute
* Accidentally accessing offensive or pornographic material and failing to report the incident
* Deliberately trying to access offensive or pornographic material

**Communications Policy**

**Introducing the e-safety policy to pupils**

* E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year
* Pupils will be informed that network and Internet use will be monitored
* Pupils will take part in Safer Internet Day (February of each year) to promote safer and more responsible use of online technology

**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’ support**

* Parents’ attention will be drawn to the School e-Safety Policy in newsletters, the school handbook and on the school website
* E-safety workshops will be held for parents and children to learn about internet safety.

**Policy compiled by:** Monwara Rahman

**Reviewed:** October 2016

**Next review date:** October 2017