E-SAFETY POLICY

WAKEFIELD METHODIST (VC)
J, I & N SCHOOL
WITH COMMUNICATION RESOURCE

Agreed: April 2019

Review Date: April 2020

E-Safety

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience. This will include current new technology and how we should behave when using them.

The school's Online/e-safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Date Protection and Security.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from MINT network including the effective management of filtering.
- National Education Network standards and specifications.

School e-Safety Policy

Writing and reviewing the e-safety policy. The e-Safety policy relates to other policies including those for computing, Bullying and for Child Protection

- The computing co-ordinator and the Headteacher regularly review the e-safety policy.
- Our e-Safety Policy has been written by the school, building on government guidance. It has been agreed by all staff and approved by governors.
- The e-Safety Policy and it implementation will be reviewed annually.
- Approved by governors

Teaching and Learning

Why Internet use is important

- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students 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 will be designed expressly for pupil use and will include filtering appropriate to the age of the 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 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 systems security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- E-mail
- Pupils may only use approved e-mail accounts on the school system.
- 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.
- E-mail sent to an external organisation should be written carefully and authorised 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 Web site should be the school address number. Staff or pupils personal information will not be published.
- The Headteacher will take overall editorial responsibility.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully.
- Pupils full names will not be used anywhere on the Web site.
- Written permission from parents or carers will be obtained before information is published on the school web site.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any pupils or their location.
- Pupils and parents will be advised that the use of social networking is appropriate for primary aged pupils.

Managing filtering

- The school will work with LA, DfE and the MINT to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported.
- Staff will ensure that regular checks are made.

Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupil's age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the school is allowed.
- Mobile phones are not allowed on school premises. The sending of abusive or inappropriate text messages is forbidden.
- No member of staff should use their personal (ie Other than Wakefield LEA) e-mail address for contact with pupils, parents or governors on School related matters.
- Staff have been advised on appropriate personal security measures when using the internet or personal mobile phones.

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 ICT Use Agreement’ before using any school ICT resource.
- 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.
- At Key stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

Assessing Risks

- The school with 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 the material will never appear on a school computer. The school cannot 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

- Incidents will be logged in the ICT incidents folder located in the office.
- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Headteacher
- Complaints of a child protection nature must be dealt with school child protection procedures.
- Pupils and parents will be informed of the complaint procedure.

Communication 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.
- Staff and the e-Safety Policy
- All staff will be given the e-Safety policy and its importance explained.
- Staff should be aware that the Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents support

- Parent's attention will be drawn to the e-Safety Policy in newsletters, the school brochure and on the web site.