E-safety Policy

Issued: November 2014

Date of Review: November 2016

Headteacher: Russell Leigh _____

Chair of Governors: Duncan Lochhead _____

Our e-Safety Policy has been written following government guidance.

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 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 will be updated regularly.
- Security strategies will be discussed with Oxfordshire.

Published content and the school website

- 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 Staff or pupils' personal information will not be published.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 will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- 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.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Websites were opportunities to upload videos, i.e. YouTube will be restricted.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

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 Head Teacher.
- Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- If filtering methods are ineffective, additional filters will be created by our IT Technician.

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 normally be allowed in school except in exceptional circumstances. Permission will need to be given by the Head Teacher. 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.

Policy Decisions

Authorising Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- At Key Stage 1, access to the Internet will be with adult supervision on specific, approved on-line materials.
- Parents will be asked to sign and return a consent form regarding internet usage when their child starts school.

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 OCC 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 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.
- In serious cases of misuse discussions will be held with the appropriate agencies e.g. child protection.

Community use of the Internet
- The school will liaise with local organisations to establish a common approach to e-safety.

Communications Policy
Introducing the e-safety policy to pupils
- E-safety rules will be highlighted to all pupils at least once every term.
- Pupils will be informed that network and Internet use will be monitored.

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 prospectus and on the school website.

Failure to Comply
- Failure to comply in any way with this policy will be considered a serious risk to health & safety and all incidents of non-compliance will be investigated by a senior member of staff.