Online Safety Policy

Introduction

Online Safety is not just about keeping safe on the internet, but includes being safe when using all electronic devices including mobile phones, tablets and television.
The Online Safety Policy links to other school policies including those for Computing and Safeguarding including Child Protection, Anti-Bullying, Health and Safety.

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 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. All pupils are required to access the World Wide Web on a regular basis.

Internet Use.

Internet use enhances learning throughout the school. The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Pupils are taught what internet use is acceptable and what is not, and given clear objectives for safe internet use.

Pupils are taught how to use the internet effectively for research, including the skills of knowledge location, retrieval and evaluation. Pupils are 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 http://www.copyrightsandwrongs.nen.gov.uk/schools-a-copyright

Managing Internet Access

The School ICT systems' capacity and security is reviewed regularly. Virus protection is updated regularly.

Security strategies are monitored by the school Network Manager, Computing Subject Leader, Online Safety governor and the leadership team. Pupils may only use approved authorised email accounts - group or individual - that are part of the school network. Pupils are not to use their own personal/family accounts.

Pupils must immediately tell a teacher if they receive offensive email. Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone.

Pupils who send emails 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 website

The contact details on the school website should be the school address, email 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 Staff or pupils' personal information will not be published.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 to the best of their ability.

Publishing pupils' images and work

Photographs that include pupils are selected carefully. Pupils' full names, and other personal details that can identify a child, will not be used anywhere on the website or twitter, particularly in association with photographs.

Written permission from parents or carers is obtained before photographs of pupils are published on the school website or twitter on admission to the school, as part of the Online Safety Agreement.

The school retains all intellectual rights to any school-related work published.

Social networking and personal publishing

The school will block / filter access to all social networking sites. News groups are blocked unless a specific use is approved. Pupils are advised never to give out personal details of any kind which may identify them or their location.

Pupils and parents are advised that the use of social network sites outside school is inappropriate for primary aged pupils.

Managing filtering

The school will work with the local authority and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If pupils discover an unsuitable site, it must then be reported to a member of staff who in turn should refer the matter to the Computing Subject Leader or Head Teacher. If staff access an unsuitable site then the Network Manager should be informed immediately. In both cases, the Network Manager will arrange for access to the site to be blocked. Children are taught what to do if an unsuitable site or 'pop-up' appears on the screen (click on the dolphin icon and report immediately to the teacher, who will obtain the address and report to the Network Manager as above). The Network Manager will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. The Network Manager will keep a log of all incidents. During KS2 pupils will be taught how to report unpleasant internet content by using the Child Exploitation and Online Protection (CEOP) 'Report abuse' icon. (A link is available on our the school's website)

Managing new and emerging technologies (including mobile phones and iPads)

New and emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed. The use of portable media such as memory sticks and CD ROMS is monitored closely as potential sources of computer virus and inappropriate material.

Pupils are not allowed to bring mobile phones to school. If they do, the mobile phone is confiscated by teaching staff at morning registration and returned to the pupil's parent at the end of the school day.

The school accepts no responsibility for loss or damage to pupils' phones however caused. Being in possession of a mobile phone during school time is in breach of the school discipline policy. The sending of abusive or inappropriate text messages is forbidden.

Staff will only use a school phone where contact with pupils or parents/carers is required.

Staff should not use personal mobile phones during the school day, unless in an emergency and only with permission from the Head Teacher.

Staff are permitted to use mobile phones in designated private non-teaching areas (e.g. personal office, staffroom) during breaks.

The Senior Leadership Team ensure that any mobile device accessing the internet on the school site via wired or wireless connection will be subject to default pupil filtering to prevent access to undesirable material and communication. This is achieved by a firewall managed by 'Talk Straight'.

Protecting personal data

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

Policy decisions

Authorising Internet access

Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Pupil Online Safety Rules and Internet Agreement. (Appendix 2 of The Acceptable Use of the Internet Policy) These Online Safety rules will also be displayed clearly all around school, in classrooms and in all networked rooms. Failure to abide by these rules may constitute a breach of the school discipline policy.

Where possible, all pupil access to the internet is supervised by an adult, using approved on-line materials. Older children (upper key stage 2, and at the discretion of the teacher) will on occasions be indirectly supervised if they are completing an independent task, set by the teacher.

All parents/carers are asked to sign the parent/carer Internet Agreement confirming that they will comply with this policy ensuring that their child follows to the best of his or her ability the school Online Safety rules.

All staff must read and agree in writing to adhere to the Internet Agreement for Staff before using any school ICT resource.

All children in Key Stage 2 are issued with a username and password to access emails. Children are taught the importance of keeping their passwords secure.

Assessing risks

The school's Senior Leadership Team take on the responsibility to monitor, evaluate and assess risk regarding Online Safety.

The school takes 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. The school cannot accept liability for the material accessed, or any consequences of Internet access, however caused.

The school will audit Computing provision regularly to establish if the Online Safety Policy is adequate and that its implementation is effective.

Handling Online Safety complaints

Complaints about Internet misuse are 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. A copy of the school complaints' procedure is available on request and is also on the website.

Community use of the Internet

External organisations using the school's Computing facilities must adhere to the Online Safety Policy.

Communications Policy

Introducing the Online Safety Policy to pupils is completed at the start of each year and during Online Safety week.

Online Safety rules are posted in all Classrooms, around school and in all networked rooms. They are discussed with the pupils at the start of each year and periodically throughout the year via their Computing curriculum. Pupils are informed that network and internet use is monitored.

Staff and the Online Safety Policy

All staff are given a copy of the School Online Safety Policy and are expected to have read it and understood its contents. Any information downloaded must be respectful of copyright, property rights and privacy. Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Laptops and iPads issued to a member of staff remain the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to internet access, data protection and use of software.

Enlisting parents' support

Parents'/Carers' attention is drawn to the school Online Safety policy in newsletters and the school website. Parents/Carers are given opportunities to attend workshops and are provided with additional leaflets and/or information regarding Online Safety guidance.

Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the Computing Subject Leader, the Network Manager, the DSL and the Senior Leadership team and the Online Safety leader

This policy is the Governors' responsibility and they review its effectiveness annually. They do this during reviews conducted between the Network Manager, Computing subject leader, Designated Senior Leader for Child Protection, Governor with responsibility for Online Safety and Governor with responsibility for Safeguarding.

Ongoing incidents are reported to the Local Governing Body.

Date agreed by the Governing Body: 4/12/17

Signed: David Duff

(Chair of the Governing Body)