E SAFETY POLICY

Teaching and learning

Why the Internet and digital communications are important

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. This is now referred to as óDigital Literacyô in the new curriculum document.

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 shown how to publish and present information to a wider audience.

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 will be taught the importance of cross-checking information before accepting its accuracy.

Pupils will be taught how to report unpleasant Internet content.

Managing Internet Access
Information system security

School COMPUTING systems security will be reviewed regularly.

Virus protection will be updated regularly.

Security strategies will be discussed with the Local Authority.

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.

In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Outgoing e-mail from pupils to external bodies will be presented in a standard manner with appropriate automatic signatures.

The forwarding of chain letters is not permitted.

Published content and the school web site

Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office.

The Head Teacher 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 so that individual pupils cannot be identified or their image misused.

Pupilsô full names will not be used anywhere on a school Web site or other on-line space, 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.

Work can only be published with the permission of the pupil and parents/carers.

Pupil image file names will not refer to the pupil by name.

Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories

Social networking and personal publishing

The school will control access to social networking sites, and consider how to educate pupils in their safe use.

Newsgroups will be blocked unless a specific use is approved.

Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.

Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for all pupils.

Pupils will be advised to use nicknames and avatars when using social networking sites.

Managing filtering

The school will work with Nottinghamshire County Council, the EMBC Broadband Consortium and Naace to ensure systems to protect pupils are reviewed and improved.

If staff or pupils come across unsuitable on-line materials, the site 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 videoconferencing & webcam use

Videoconferencing will use the educational broadband network to ensure quality of service and security.

Pupils must ask permission from the supervising teacher before making or answering a videoconference call.

Videoconferencing and webcam use will be appropriately supervised for the pupilsô 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 in school by students. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.

Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. The use of such equipment requires the express consent of a member of the Senior Leadership Team.

Students are not allowed use of their phones, iPads and other tablets containing images or any video footage without prior permission from form teacher.
The form teacher will only give permission for the use of such equipment if the images or video footage are deemed relevant to the educational topics in question.

Staff will be issued with a school phone where contact with pupils is required or where mobile phones are used to capture photographs of pupils.
Staff must not use their own personal phones to capture studentsô images or videos.

The use of a Learning Platforms will be developed over the next 12 months and parents/carers provided with specific e-safety considerations as necessary.

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 óStaff Code of Conduct for COMPUTINGô before using any school COMPUTING resource.
The school will maintain a current record of all staff and pupils who are granted access to school Computing systems.

As appropriate for individuals/groups, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

Parents will be asked to sign and return a consent form.

Any person not directly employed by the school will be asked to sign an óAcceptable use of school Computing resourcesô before being allowed to access the internet from the school site.

Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor NCC can accept liability for any material accessed, or any consequences of Internet access.

The school will audit Computing use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Prevent Duty Guidance
The school will ensure children are safe from terrorist and extremist material when accessing the internet within the premises, including by establishing appropriate levels of filtering.

The school will also advise parents on options for internet filtering at home, in order to compliment the monitoring and enforcement of Prevent policy put in place by the school.

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 (see schools complaints policy)

Pupils and parents will be informed of consequences for pupils misusing the Internet.

Communication Policy

Introducing the e-safety policy to pupils

Pupils will be informed that network and Internet use will be monitored and appropriately followed up.

e-Safety training will be embedded within the Computing scheme of work or the Personal Social and Health Education (PSHE) curriculum.

Pupils need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

Pupils should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the schoolôs e-safety policy also covers their actions out of school, if related to their membership of the school.

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.

Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.

Staff that manage filtering systems or monitor Computing use will be supervised by senior management and work to clear procedures for reporting issues.

Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

Parentsô and carersô attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

The school will maintain a list of e-safety resources for parents/carers.

The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Reviewed May 2017