NUNTHORPE PRIMARY ACADEMY

ONLINE-SAFETY

Approved by Full Governing Body 07.03.16

Date of next review Spring 2017

Signed by _____ _____

Mr G Greer **Mrs A O'Gara**

Chair of Governors **Head Teacher**

WRITING AND REVIEWING THE E-SAFETY POLICY

The Online-safety Policy is part of the Academy Development Plan and relates to other policies including those for ICT, bullying and safeguarding.

- The Academy will appoint an Online-Safety Leader. This may be the Designated Child Protection Co-ordinator as the roles overlap.
- Our Online-Safety Policy has been written by the Academy, building on the Redcar & Cleveland Local Authority Online-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The Online-Safety Policy and its implementation will be reviewed annually.
- The Online-Safety Policy was revised by Mr Salter & Mrs O'Gara.
- The Online-Safety Policy was approved by the Governors in Spring 2017.

WHY INTERNET USE IS IMPORTANT

The Internet is an essential element in 21st Century life for education, business and social interaction. The Academy has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

INTERNET USE WILL ENHANCE LEARNING

The Academy Internet access will be designed and managed specifically 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 Academy 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.

PUPILS WILL BE TAUGHT BASIC RULES ON INTERNET SAFETY

Teachers will regularly remind pupils and parents of how to keep themselves safe on the Internet, so that they have the knowledge and understanding to apply this outside the Academy as well as in it.

INFORMATION SYSTEM SECURITY

Academy ICT systems capacity and security will be reviewed regularly.

Virus protection will be upgraded regularly.

Security strategies will be discussed with the IT Provider.

E-MAIL

Pupils may only use approved e-mail accounts on the Academy 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-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on Academy headed paper.

The forwarding of chain letters is not permitted.

PUBLISHED CONTENT AND THE ACADEMY WEB SITE

The contact details on the web site should be the Academy 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 the content is accurate and appropriate.

PUBLISHING PUPILS' IMAGES AND WORK

Photographs that include pupils will be selected carefully and will be displayed with parental consent.

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 Academy website.

SOCIAL NETWORKING AND PERSONAL PUBLISHING

The Academy 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 kind which may identify them or their location.

Pupils and parents will be advised that the use of social networking spaces (such as Facebook, Twitter etc.) outside school is inappropriate for primary aged pupils.

MANAGING FILTERING

The Academy will work with our ICT Technician, DoE and the IT support provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover and unsuitable site, it must be reported to the Head and Deputy. A record of any occurrences will be kept on CPOMs.

The Head Teacher and Deputy Head Teacher will ensure that regular checks are made by the IT provider to ensure that the filtering systems are appropriate and effective. Any misuse (such as searching for age inappropriate material or material associated to radicalisation) is reported to The Head and Deputy and dealt with appropriately.

MANAGING EMERGING TECHNOLOGIES

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the Academy is allowed.

Pupils will not be allowed to bring mobile phones into the Academy, unless a parent specifically requests it. If a mobile phone is requested it should be handed over to the class teacher at the beginning of the day for safe keeping.

The sending of abusive or inappropriate text messages is forbidden.

Electronic devices such as iPads may be brought into the Academy to share homework.

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 Academy ICT resource.

The Academy 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 pupils' access may be withdrawn.

In EYFS and 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 when their child starts at the Academy.

Assessing risks

The Academy 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 an Academy computer. Neither the Academy nor the LA can accept liability for the material accessed, or any consequences of Internet access.

The Academy will audit ICT provision to establish if the Online-Safety Policy is adequate and that its implementation is effective.

Handling Online-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 Academy 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.

Community use of the Internet.

The Academy will liaise with local organisations such as Redcar & Cleveland Group for online-safety and South Tees Local Safeguarding Children Board, to establish a common approach to online-safety.

COMMUNICATIONS POLICY

Introducing the Online-Safety policy to pupils

Online-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 ONLINE- SAFETY POLICY

- All staff will be given the Academy Online-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.

ENLISTING PARENTS' SUPPORT

Parents' attention will be drawn to the Academy Online-Safety Policy in newsletters, the Academy brochure and on the Academy Website.

MOBILE PHONE POLICY

- As a general rule, staff should not make and receive calls, or send texts, or access social media except at lunch time or during breaks.
- Mobile phones should be turned off, or be on silent, while the employee is at work.
- If there is a specific reason to keep a mobile phone on for a limited time, staff may request permission for this from the team leader.
- Phones should generally be stored away from view.
- A school device should be the preferred option to take photographs and videos of students.
- The Head and Deputy Head teacher use a mobile phone to take photographs for the school Twitter account using the Twitter app. This material is usually then deleted. These mobile phones are checked during termly supervision from our Safeguarding Consultant.
- If staff use the camera on their mobile phones to take photographs or videos of students this should be saved on a school device and deleted from the personal device as soon as possible.
- Employees are encouraged not to use their phones in the classroom, playground, or any other area where pupils are present unless it is to enhance a lesson.
- The school mobile phone may be used by the Head Teacher for personal use; as agreed by the Governing Body.