E-Safety Policy

Safeguarding Statement

Everyone at Horton Grange shares an objective to help keep children and young people safe by contributing to:

- Providing a safe environment for children and young people to learn in school and;
- Identifying children and young people who are suffering or likely to suffer significant harm, and taking appropriate action with the aim of making sure they are kept safe both at home and in school.

Reviewed date: September 2017
Next review date: September 2018

Headteacher – Nichola Irving
E-Safety Co-ordinator – Caroline Ash
Deputy E-Safety Co-ordinator - Amanda Tartt
E-Safety Governor – Karl Lunn
Chair of Governors – Janet Dyson
Safeguarding Governor – Peter Standfield
ICT Technician – John Harwood
ICT Subject Leaders – Hamish Fields/Judi Crumley/Beth Robinson

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, IPADs, collaboration tools and personal publishing.

The school's E-Safety policy will operate in conjunction with other policies

- Behaviour
- Anti-bullying
- Child protection
- Curriculum
- Data Protection
- Photography
- Preventing extremism and radicalisation
- Social networking policy and guidance
- IT Security Policy

E- Safety relies 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 including the effective management of filtering;
- The appointment of an E-Safety co-ordinator and deputy to implement and manage this policy;
- The support of the headteacher and governing body;
- Supporting parents in the use of ICT and emerging technologies at home.

1. Introduction

The purpose of this policy is to:

- Establish ground rules that are in place in Horton Grange Primary School for using the internet and electronic communications such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate the pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience;
- Describe how these fit into the wider context of our discipline and PSHE policies;
- Demonstrate the methods used to protect children from accessing sites containing inappropriate material such as pornography, racist or politically extreme views and violence;
- To be reviewed regularly and in the light of new technologies. This will be carried out with the involvement of staff, pupils, governors and parents.

The Role of the E-Safety Co-ordinator

- The E-safety Co-ordinator is responsible for regularly monitoring internet and device use and updates the head teacher, governors and senior managers on a regular basis.
- The E-Safety Co-ordinator acts as a point of contact for E-Safety issues within the school.
- The E-safety Co-ordinator supports the national E-Safety strategy and disseminates up to date information among the staff and arranges staff development as a result of information regarding emerging and changing technologies.
- The E-Safety Co-ordinator is also jointly responsible along with the Designated Person for Child Protection and Safeguarding Co-ordinator for the duty of care requirements under the Safeguarding arrangement within school.
- The E-Safety Co-ordinator is supported in this role by the Deputy E-Safety Co-ordinator.

2. Teaching and Learning

- The internet is an essential element in 21st century life for business and social interaction. The school has a duty to provide children and staff with quality internet access as part of the learning experience.
- Internet access is part of the statutory curriculum and a necessary tool for students and staff
- The school's curriculum internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils through the installation of Policy Central Enterprise (PCE) provided by the LA.
- Pupils are taught about acceptable internet use and are given clear objectives for internet use.
- As part of each year group's curriculum, pupils will be taught all areas of E-Safety. We hold an annual safety week where issues around all aspects of E-Safety are covered and further issues are addressed as they arise.
- Pupils and staff are expected to acknowledge and agree to the acceptable use policy when logging onto the curriculum system with their individual passwords.
- Pupils are taught about effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school ensures that the use of the internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught what to do if they come across or receive offensive or unpleasant material whilst using technologies through reporting to teachers/parents, or using the 'report' button on internet sites at home.
- Staff are trained in the use of new technologies including any associated possible safety issue as they arise.
- Staff are aware of how to report instances of unsuitable material using the E-Safety incident guidelines provided by NCC.

3. Using Technologies

- The school's curriculum ICT system is monitored by PCE which sends weekly updates to the E-Safety Co-ordinator regarding unacceptable use of the system. This identifies individual pupils, staff or computers which have been used and reports on the types of inappropriate access. This can then be managed according to the school's behaviour policy.
- Mobile devices (IPADs) have Lightspeed recommended firewalls installed on them which are regularly updated if the internet is accessible on the devices. This monitors all internet activity.

- Virus protection is updated regularly by the ICT Technician.
- Staff are not permitted to access the school's wireless technology with their person laptops unless PCE is installed.
- Staff using school laptops at home are aware that PCE is installed on all units and that the appropriate use of the equipment will be monitored when the laptop accesses the school's wireless system on its return to school.

E-Mail

- Pupils may only use approved e-mail accounts on the school system where available (eg School 360).
- Pupils must immediately tell a teacher if they receive offensive material or comments via email.
- Pupils are taught not to reveal personal details of themselves or others in electronic communication, or arrange to meet anyone.
- E-mail sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper
- Staff should, wherever possible, use the admin email address for contacting parents. Personal or NCC email addresses should not be used to contact parents without discussing the implications of this with the E-safety Co-ordinator/ headteacher. If parents make contact through the county email system, this should be reported to the E-Safety Co-ordinator.
- Under no circumstances should staff issue personal or work email addresses to pupils or contact pupils.

School Website

- The contact details on any school website should be the school address, email and telephone number. Staff and pupil details or personal information is not to be published.
- The headteacher has overall editorial responsibility and ensures that the content is accurate and appropriate.
- Photographs that include pupils are selected carefully so that they do not enable individual children to be clearly identified.
- Pupil's full names are not used anywhere on the website.
- Written permission from parents/carers must be obtained before photographs of pupils are published on the website. This is done on an annual basis for that academic year. Any parent who wishes to withdraw this permission should contact the school office.

Social networking and personal publishing

- Any social network sites used to support learning or links with other schools must be secure. They must be approved by the headteacher before use and any content uploaded should be checked by the teacher. The teacher is also responsible for pre-checking any content to be viewed by the children.
- The school blocks access to public social networking sites. Newsgroups are also blocked.
- Pupils are told never to give information which may allow them to be identified.
- Parents are invited to e-safety events which advise that the use of social network sites (as well as other digital media) outside school brings a range of dangers for primary aged pupils.
- Parents are given the opportunity to suggest training or information requirements that they may have regarding E-Safety.
- Staff are provided with guidance to support their safe use of social networking sites out of school through the Staff Social Network policy and County Council Guidelines.

Mobile Phones and Mobile Devices

- In order to ensure the safety of both children and staff, mobile phones and other mobile devices should not be visible in the vicinity of children during the school day. Mobile phones should not be used during teaching sessions. If it is felt necessary to make phone calls/take messages during the school day this must occur during lunch / break times in an areas where there are no children (eg empty classroom/staff room). This is to safeguard teachers as well as pupils.
- Staff should, wherever possible use the school mobile phone when off site.
- Staff should not give out personal mobile numbers to pupils.
- Pupils are not permitted to bring mobile phones and other devices with photographic/video capability (eg ipods) into school except with the express permission of the Headteacher/senior staff.
- Pupils in Year 4 who begin walking home unaccompanied will be allowed to bring phones into school for their safety if parents read and sign the mobile phone policy. This will be on the understanding that the phones will not be turned on while on the school premises, are kept by the teacher in a safe place and are brought in at the owners' risk. Infringement of these rules will result in the phone being confiscated for the duration of the school day and parents contacted.
- As part of the children's e-safety education, children are taught how to respond in the instance of receiving malicious messages or texts.

Photographs

- Photographs/videos taken during school trips should only be taken by staff members on cameras which are directly downloaded into the appropriate folder on the school network. This should be school cameras wherever possible.
- Photos should not be taken on devices that have internet or Bluetooth technology.
- If pupils use the school cameras, the teacher responsible for the group should supervise the shot where possible.
- Parent volunteers on trips are instructed that they are not allowed to take photographs on their mobile phones.
- All photographs taken by children and staff should be scrutinised by the teacher for suitability before being used for any purpose.
- All photographs/videos should be viewed by the teacher for appropriateness before publishing openly. Photographs which may cause the subject to be embarrassed or upset should be deleted. Any child taking photographs deemed to be inappropriate should be dealt with in terms of the behaviour or bullying policy as appropriate.

4. Managing Technologies

Emerging technologies are evolving at a rapid rate and although every attempt is made to protect children from offensive or inappropriate material and misuse, there may be occasions when inadvertent access occurs. The following points apply:

- If staff or pupils discover an unsuitable site, it must be reported immediately to the teacher and then the E-Safety Co-ordinator, who will report the site to the appropriate person in the local authority (Richard Taylor/John Devlin) according to the safety incident flow chart displayed in the staff room. Following the flow chart, if it is felt that the incident is a child protection issue; this will immediately be reported to the headteacher and LCSB as necessary.
- If an incident involves extremist material, the Police should also be notified as well as the LSCB if it is felt that the access has been deliberately sought.

- All internet access including emails will be monitored through PCE on the curriculum network. The admin system is protected by a separate firewall system.
- Regular updates from the local authority providing guidance for the safe use of technologies are acted on as it is received.

5. Policy Decisions

- All staff and pupils must agree to the acceptable use policy in ICT agreement which forms part of the staff induction process and on the desktop screen following the login procedure.
- The AUP is regularly explained to the children at their level to ensure their understanding.
- The AUP is included in the home/school agreement to ensure that parents are aware of the high priority that the school places on safe use of technologies. It is also displayed in areas where computers are present.
- PCE reports are regularly monitored by the E-Safety Co-ordinator who in turn reports to the senior management.
- The school keeps a record of all staff and pupils who are granted internet access.
- At key stage 1 /Early Years, access to the internet will be by adult demonstration with directly supervised access to approved online materials.
- At KS2, access to the internet will be by supervised access to online materials filtered by PCE.

6. Assessing Risks

- The school takes all reasonable precautions to ensure that users access only appropriate material through the use of PCE systems. Supervised access is recommended as the school is aware that no firewall system is completely infallible.
- The school audits ICT provision on an annual basis, or when new technologies are introduced to establish if the e-safety policy is adequate and that its implementation is effective

7. Handling E-Safety Complaints

- The E-Safety Co-ordinator will inform class teachers if it is felt that there has been an infringement of the AUP by a child in the class. Minor infringements will first result in a warning given to the child. Further or more serious infringements will be dealt with under the school's behaviour policy.
- Any infringement of the school policy by pupils or staff which is deemed to be a child protection issue will immediately be reported to the appropriate authorities. Where this involved a member of staff, disciplinary procedures will be instigated.
- Incidents where staff or pupils are suspected of having obscene images on a mobile device will be dealt with via the NCC flow chart system and via the disciplinary procedures.

This policy will be reviewed in September 2018 (or earlier if legislation, guidance or circumstances dictate)