STANHOPE BARRINGTON
C OF E PRIMARY SCHOOL

E-SAFETY POLICY

Who will write and review the policy?

The e-safety policy is part of many different schools policies including the ICT Acceptable Use policy, Child Protection or Safeguarding Policy, Anti-Bullying and School Improvement Plan and should relate to other policies including those for behaviour, for personal, social and health education (PSHE) an for citizenship. Policy construction provides a method to review practice – in this case the use of technology and its benefits and risks. The more the staff, parents, governors and pupils are involved in deciding and creating the policy the more effective it will be.

It is recommended as best practice that all schools appoint an e-safety Co-ordinator to lead on e-safety. Our school's e-safety Co-ordinator is Mrs Cross, Deputy Headteacher.

The school's Designated Child Protection Co-ordinator will need to be aware of e-safety training and resources and be available should any child wish to disclose information regarding an online incident. Therefore it may be an idea to elect them as e-safety representative. However, another member of staff may be elected. The DCPC must be made aware of any disclosures, incidents or Child Protection concerns. The Senior Leadership Team and Governing Body must be involved and should review the e-safety policy annually and monitor its impact. They will also need to ensure that they take responsibility for revising the e-safety policy and practice where necessary (such as after an incident or change in legislation).

The Headteacher and Governing Body have a legal responsibility to safeguard children and staff and this includes online activity.

- The school has appointed an e-safety Co-ordinator (Mrs D Cross).
- The e-safety policy and its implementation will be reviewed annually.
- Our e-safety policy has been written by the school, building on the DCC e-safety policy and government guidance.
- Our school policy has been agreed by the Senior Leadership Team and approved by Governors.
- Our school has formed an e-safety committee.
- The school has appointed a member of the Governing Body to take lead responsibility for e-safety.

The school e-safety Co-ordinator is: Mrs D Cross ……………………………

Policy approved by Headteacher: Mr S Myers ………………….Date:…………

Policy approved by Governing Body: Mr S Wilson (Chair) ……………………..

Date:…………………

Teaching and Learning

Why is Internet use important?

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in education through ICT and Internet use.

- Internet use is part of the statutory computing curriculum (2014) and is a necessary tool for learning.
- The Internet is a part of everyday 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.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

How does Internet use benefit education?

A number of studies and government projects have identified the educational benefits to be gained through the appropriate use of the Internet including increased pupil attainment.

Benefits of using the Internet in education include:

- Access to worldwide educational resources including museums and galleries.
- Educational and cultural exchanges between pupils worldwide.
- Vocational, social and leisure use in libraries, clubs and at home.
- Access to experts in many fields for pupils and staff.
- Professional development for staff through access to national developments, educational materials and effective curriculum practice.
- Collaboration across networks of schools, support services and professional associations.
- Improved access to technical support including remote management of networks and automatic system updates.
- Exchange of curriculum and administration data with DCC and DfE.
- Access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Increased computer numbers and improved Internet access may be provided but its impact on pupils learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights and the correct use of published material should be taught. Methods to detect plagiarism may need to be developed.

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- The school will ensure that the copying and subsequent use of Internet derived material by and pupils complies with copyright law.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils will be educated in effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

Managing Information Systems

How will information systems security be maintained?

It is important to review the security of the whole system from user to Internet. This is a major responsibility that includes not only the delivery of essential learning services but also the personal safety of staff and pupils.

ICT security is a complex issue which cannot be dealt with adequately within this document. A number of agencies can advise on security including DCC and network suppliers.

How will email be managed?

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission from an adult.
- Staff will only use official school provided email accounts.
- Access in school to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and will be restricted.
- Email sent to external organisations should be written on school headed paper, be written carefully and authorised by an adult before sending.
- The forwarding of chain messages is not permitted.
- Staff should not use personal email accounts during school hours or for professional purposes.

How will published content be managed?

Many school have created excellent websites and communication channels, which inspire pupils to publish work of a high standard. Websites can celebrate pupil's work, promote the school and publish resources for projects. Editorial guidance will help reflect the school's requirements for accuracy and good presentation.

Sensitive information about schools and pupils could be found in a newsletter but a school's website is more widely available. Publication of any information online should always be considered from a personal and school security viewpoint. Material such as staff lists or a school plan may be better published in the school handbook or in a secure part of the website which requires authentication.

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The Headteacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate.
- The school website will comply with the school's guidance for publications including respect for intellectual property rights, privacy policies and copyright.

Can pupils' images or work be published?

- Images or videos that include a pupil will be selected carefully and will not provide material that could be reused.
- Pupil's full names will not be used anywhere on the website, particularly in relation to photographs.
- Written permission from parents or carers will be obtained before images/videos of pupils are electronically published.
- Pupils work can only be published with their permission or their parents.
- Written consent will be kept by the school where pupils' images are used for publicity purposes, until the image is no longer in use.

How will social networking, social media and personal publishing be managed?

- The school will control access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and or their location.
- Staff wishing to use social media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those which may be considered threatening, hurtful or defamatory.
- Newsgroups will be blocked unless a specific use is approved.
- Concerns regarding pupils' use of social networking, social media and personal publishing sites (in or out of school) will be raised with parents/carers, particularly with regard to underage use of sites.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the ICT Acceptable Use Policy.

How will filtering be managed?

Most Durham schools have three possible models for changing the default filtering settings:

1. Authorised only by the Headteacher by contacting the ICT Service desk with their PIN Number.
2. Other staff can be delegated permission to change the filtering by contacting the ICT Service desk with their PIN Number.
3. Access can be changed directly by authorised people within the school by connecting to the website.

In all cases it is important to establish a protocol for establishing the responsibility for checking a site which needs changes to the filtering.

- If a contentious website is requested (e.g. Youtube) it will be discussed by the e-safety committee.
- For other sites the responsibility for checking the suitability of the site rests with the teacher requesting access.
- The school's broadband will include filtering.
- The school will have a system in place to make changes to the filter, including who is responsible for authorising changes.
- The school will work with DCC to review filtering.
- The school will have a clear procedure for reporting breaches of filtering.
- If staff or pupils discover unsuitable sites, the URL will be reported to the school e-safety Co-ordinator who will then record the incident and escalate the concern as appropriate.
- The school filtering system will block all sites on the Internet Watch Foundation (IWF) list.
- Changes to the school filtering policy will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Durham Police or DCC.

How will videoconferencing be managed?

Stanhope Barrington CofE Primary School do not currently participate in videoconferencing.

How are emerging technologies managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils are allowed to bring a mobile phone to school but must hand it into their class teacher at the beginning of the school day.
- Pupils are taught about the appropriate and inappropriate use of personal devices both at school and at home.
- Staff all sign an Acceptable Use Policy which prohibits the use of mobile devices during teaching time or in front of children.

How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The School has a Data Protection Policy.

Policy Decisions

How will Internet access be authorised?

- All staff will read and sign the School Acceptable Use Policy before using any school ICT resource.
- Parents will be asked to give consent for their child to use ICT within school.
- All visitors to the school site who require access to the school network will be asked to read and sign the Acceptable Use Policy.

- Parents will be informed that pupils will be provided with supervised Internet access appropriate to their age and ability.
- When considering access for vulnerable members of the school community (such as children with special educational needs or disabilities) the school will make decisions based on the individual needs of the child.

How will risks be assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer or device. Neither the school or DCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of the computer systems without permission or for inappropriate purposes could constitute offence under the Computer Misuse Act 1990 and breaches may be reported to the police.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will the school respond to incidents of concern?

- All members of the school community will be informed about the procedure for reporting e-safety concerns (such as breaches of filtering, cyberbullying, illegal content, etc.).
- The e-safety co-ordinator will record all reported incidents and actions taken in the School e-safety incident log.
- The Designated Child Protection Coordinator will be informed of any e-safety incidents involving Child Protection concerns.
- The school will manage e-safety incidents in accordance with the school disciplinary/behaviour policy where appropriate.
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Children's Safeguarding Team or e-safety officer and escalate the concern to the police.
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-safety Officer.

How will e-safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the school's complaints procedure.
- Any complaint about staff's misuse will be referred to the Headteacher.
- All e-safety complaints and incidents will be recorded by the school, including any actions taken.
- Parents and pupils will be informed of the complaints procedure.
- Any issues will be dealt with via the school's disciplinary, behaviour and child protection procedures.

How will cyberbullying be managed?

Cyberbullying is defined as: "The use of Information Communication Technology, particularly mobile phones and the Internet to deliberately hurt or upset someone" DCSF 2007.

There are a number of statutory obligations on schools with regard to behaviour which establish clear responsibilities to respond to bullying. In particular, section 89 of the Education and Inspections Act 2006:

- Every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's behaviour policy which must be communicated to all pupils, school staff and parents.
- It gives Headteachers the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff.
- Cyber bullying of any members of the school community will not be tolerated.
- There are clear procedures in place to support anyone in the school community affected by cyber bullying.
- All incidents of cyber bullying reported to school will be recorded.
- There are clear procedures in place to investigate incidents or allegations of cyberbullying.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-safety poliy.
- Sanctions for those involved in cyberbullying may include:
  - The bully will be asked to remove any material deemed to be inappropriate or a service provider may be contacted to remove content if the bully refuses or is unable to comply.
  - Internet access may be suspended at school for the user for a period of time.
  - Parents/ carers will be informed.
  - The police will be contacted if a criminal offence is suspected.

How will mobile phones and personal devices be managed?

Pupils Use of Personal Devices

- Pupils may not use mobile phones in school. If a child brings a mobile phone into the school then it must be handed to the Class Teacher before the start of the school day.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a phone or device if they believe it is being used to contravene the school behaviour/bullying policy. The phone or device may be searched by the School Leadership Team and may be handed over to the police if necessary.

Staff use of Personal Devices

- Staff mobile phones will not be used when children are present and will be stored safely during lesson times.
- Staff are not permitted to use their own personal phones or devices for contacting children or their families within or outside of the setting in a professional capacity.
- Mobile phones and devices will be switched off or switched to silent mode. Bluetooth communication should be hidden or switched off and devices will not be used in lesson time unless permission has been given by the Senior Leadership Team in emergency situations.
- Staff should not use personal devices to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.