Stephenson Way Community Primary School – E-Safety Policy 2013

Who will write and review the policy?

- The school will appoint an e–Safety Coordinator. At the time of writing this policy, the e-safety co-ordinator is the Deputy Headteacher.
- The e–Safety Policy and its implementation will be reviewed annually.
- Our e–Safety Policy has been written by the school, building on government and county guidance. It has been agreed by the Senior Leadership Team and approved by governors.

Why do we think Internet use important?

- Internet use is part of the statutory curriculum and 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 our pupils 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, providing they show a responsible and mature approach to its use.

How does Internet use benefit education?

We believe that the benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between pupils world-wide
- 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
- Access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- The school's Internet access is be designed to enhance and extend education.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- 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 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 are taught to be critically aware of the materials they read and view, and are shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of teaching/learning in every subject.
- Teachers will model how they as adults evaluate internet content.

How will information systems security be maintained?

- Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.
- Our Servers are located securely and physical access to them is restricted by needing a key. Our servers are updated regularly via an SLA bought from the county for a twice per month onsite technician.
- Virus protection for the whole network is installed and current, and maintained by SLA technician.
- Internet connections are arranged via the county recommended providers.
- The security of the school information systems and users are reviewed regularly.
- Unapproved software are not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The ICT Subject Leader/SLA Technician will review system capacity regularly.

How will email be managed?

- Pupils may only use approved email 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 without specific permission from an adult.
- Whole-class or group email addresses may be used in primary schools for communication outside of the school.
- Access in school to external personal email accounts may be blocked.
- Email sent by pupils to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain messages is not permitted.
- At present, pupils are not allowed to email staff – this will be reviewed in the next policy review.
- At present, staff do not email pupils - this will be reviewed in the next policy review.
- All pupils and parents must sign an acceptable use policy concerning emails:

✓ *I will only use my school email address when emailing.*
✓ *I will only send emails to people I know or who my teacher has approved.*
✓ *I will only open emails from people I know or who my teacher has approved.*
✓ *If I receive an email from somebody I don't know I will tell my teacher.*
✓ *I will only open email attachments from people I know, or who my teacher has approved.*
✓ *I will not tell other people my ICT passwords.*
✓ *I will make sure that all emails I send to other children and adults are responsible, polite and friendly.*
✓ *I will not email teachers or staff at the school unless I am told to do so.*
✓ *I will not deliberately send by email anything that could be unpleasant, nasty or rude.*
✓ *If someone else sends me something which is unpleasant, nasty or rude I will tell my teacher.*
✓ *I will not give out my own details such as my name, phone number or home address by email.*
✓ *I know that my use of emails can be checked by my teacher.*
✓ *I know that the school will contact whoever looks after me at home if I do not keep to this agreement.*
✓ *I understand that this agreement is to help keep me safe and happy while I am using emails.*

How will published content (school website) be managed?

- The contact details on the website should be the school address, email and telephone/fax number.
- Staff or pupils' personal information must not be published online.
- The Headteacher and Deputy Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- Images that include pupils will be selected carefully to ensure all pupil images published are appropriate and positive for the child.
- 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 images of pupils are electronically published.

How will filtering be managed?

- Filtering for our school will be managed primarily by the county.

- Blocked sites will be monitored by the school and where appropriate the school will request further sites to be blocked by the county filtering system.
- Our school allows pupils to use Google Images, using Google Images Safe Search setting.
- Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP.
- We encourage the children to use the Safety Dolphin to alert staff if they are uncomfortable or concerned about any internet content they are viewing.

How can emerging technologies be managed?

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

How should personal data be protected?

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

How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff have internet access via Network or by their laptops. Personal computers may only be connected to the school network once the ICT Leader or SLA technician have checked over the computer and given approval.
- All pupils are allowed internet access via a personal login to the network.
- At Key Stage 1, access to the Internet will be by adult demonstration and with directly supervised access to specific, approved on-line materials.

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. Neither the school nor DCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use regularly to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

How will e–Safety complaints be handled?

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must 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 work in partnership with staff to resolve issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

How will Cyberbullying be managed?

- Cyberbullying (along with all forms of bullying) will not be tolerated in school. Full details are set out in the school's policy on anti-bullying.
- There will be clear procedures in place to support anyone effected by Cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be 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, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include: The bully will be asked to remove any material deemed to be inappropriate or offensive. A service provider may be contacted to remove content. Internet access may be suspended at school for the user for a period of time. Parent/carers may be informed. The Police will be contacted if a criminal offence is suspected.

How will Learning Platforms and learning environments be managed?

- Our DLG is provided by the county.
- ICT Leader and staff will monitor the usage of the DLG by pupils.
- Pupils/staff will be advised on acceptable conduct and use when using the DLG.
- Only members of the current pupil, parent/carers and staff community will have access to the DLG.
- Students on placement in our school will have temporary access to the DLG.
- All users will be mindful of copyright issues and will only upload appropriate content onto the DLG.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns with content may be recorded and dealt with in the following ways: The user will be asked to remove any material deemed to be inappropriate or offensive (for example in the Chatterbox section). The material will be removed by the site administrator if the user does not comply or may be removed by the administrator without the consultation of the pupil/staff member in question. Access to the DLG for the user may be suspended. The user will need to discuss the issues with a member of SLT before reinstatement. A pupil's parent/carer may be informed.

How will the popularity of virtual communities, such as Facebook, be managed?

- Internet access to Facebook and other virtual communities is blocked at our school by the county filtering system.
- Staff, children and parents, as part of their wider e-safety training, have dedicated sessions discussing virtual online communities.
- **Staff will ensure that when using Facebook, or other social networking sites, personally outside school that they have the correct security settings enabled so that personal information cannot be accessed by non friends. Staff should not discuss school issues on social networking sites and if they should be contacted by pupils or ex pupils, they should not respond and this should be reported to the SLT as a matter of record.**
- Although Facebook and similar websites have an age limit older than the children at our school, we recognise that many children under the legal age do join these sites. We are also aware that there are some online community websites which exist especially for younger children. We feel it is appropriate therefore to educate our children about keeping themselves safe online whilst participating in these online communities. Children and staff will be educated about:
  - ✓ The differences between an online friend and a real world friend.
  - ✓ That unknown people online are strangers, just as they would be in the real world.
  - ✓ Never revealing personal information online, and what is meant by personal information.
  - ✓ Never sending photographs, webcam stills, webcam streams online unless to a family member or family friend which has been sanctioned by parents or teachers.
  - ✓ Never agree to accept photographs, webcam stills, webcam streams from an online friend/chat partner/stranger.
  - ✓ Being open and honest with parents and teachers about who you are communicating with online.
  - ✓ Never agreeing to keep a secret for an online friend/chat partner/stranger.
  - ✓ Never agreeing to meet an online friend/chat partner/stranger.
  - ✓ Telling a parent or teacher straight away if an online friend/chat partner/stranger asks for a photo, personal information, or asks to meet.
  - ✓ Telling a parent or teacher if anybody online makes you feel uncomfortable for any reason, including something rude, bad language, bullying etc.

All disclosures by staff, parents and children will be recorded and if the schools thinks it appropriate the county and the police will be informed.

Staff will never agree to keep disclosures from children secret.

How will the policy be introduced to pupils?

Useful e–Safety programmes include:

- Think U Know: **www.thinkuknow.co.uk**
- Childnet: **www.childnet.com**
- Kidsmart: **www.kidsmart.org.uk**
- Safe Social Networking: **www.safesocialnetworking.com**

These are published on our website and on our staff DLG.

- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Pupil instruction in responsible and safe use should precede Internet access.
- An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use.
- E–Safety training will be part of the transition programme across the Key Stages and when moving between establishments.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

How will the policy be discussed with staff?

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

How will parents' support be enlisted?

- Parents' attention will be drawn to the School e–Safety Policy in newsletters, the school brochure and on the school website.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting e–Safety at other attended events e.g. parent evenings, sports days.
- Parents will be requested to sign an e–Safety/email agreement.
- Information and guidance for parents on e–Safety will be made available to parents on our school website.

This policy will be reviewed July 2013