**Stanborough Primary School and Nursery**

# E-SAFETY POLICY

## 1. Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Stanborough Primary School's E-Safety Policy will operate in conjunction with other policies including those for Pupil Behaviour, Bullying, Mobile Phones and the Computing Curriculum.

The E-Safety Subject Leader for Stanborough Primary and Nursery School is: **Mrs Tiann Madden**

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and pupils; 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 internet access including effective management of content filtering.

## 2. Why is Internet Use Important?

The Internet is an essential element in 21st century 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. The Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

At Stanborough Primary and Nursery School we understand the responsibility to educate our pupils in e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom. This is done through Computing and whole school assembly sessions.

## 3. How does Internet Use Benefit Education?

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;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across 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 the Local Authority; access to learning wherever and whenever convenient.

## 4. How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes 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.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support 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.
- As pupils progress through the school into Key Stage 2 they will 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 how to report unpleasant Internet content.

**5. Authorised Internet Access**

- The internet access will include filtering provided by the Stanborough Technical Department and our firewall will prevent access to any inappropriate sites. Any breaches to security must be immediately reported to the Head Teacher, Deputy or E-Safety Subject Leader.
- The school will maintain a current record of all staff and pupils who are granted Internet access.
- User ID and passwords for staff and pupils who have left the School are removed from the system during the months of August and September.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised Internet access.
- Pupils must agree to comply with the Responsible Internet Use statement before being granted Internet access.

**6. World Wide Web**

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the e-safety coordinator who will pass the information on to the head teacher and network manager.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

**7. Email**

- The school allocates each pupil their own e-mail account. Pupils may only use approved e-mail accounts on the school system.
- Pupils must not reveal personal details of themselves or others in e-mail communication.
- Pupils must report any offensive e-mails immediately to a teacher.
- Access in school to external personal e-mail accounts may be blocked.
- The school gives all staff their own e-mail account to use for all school business. This account should be the account that is used for all school business.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Staff member's personal email addresses should never be disclosed without their express permission.

**8. Social Networking**

- The school will endeavour to block/filter access to social networking sites and newsgroups 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 will not have access to social networking sites at school, but the school will educate pupils in their safe use e.g. use of passwords.
- They will be advised to never give out personal details of any kind which may identify them, anybody else or their location.
- Pupils, parents and staff will be advised on the safe use of social network spaces
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- Staff must not communicate with students using public social networking sites such as Facebook, MySpace, Twitter, etc.
- Staff should not communicate with parents about school-based issues using public social networking sites such as Facebook, MySpace, Twitter, etc.

**9. Filtering**

- The network manager will ensure that the filtering systems of the school network are effective.
- All files downloaded from the internet, received via e-mail or on removable media (e.g. CDRom or Memory Stick) will be checked for any viruses using school provided anti-virus software before files are opened.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact the network manager immediately.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Subject Leader or Head Teacher, who will inform the network manager.

**10. Managing Emerging Technologies**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the senior management team before use in school is allowed.
- Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone on trips and off-site visits to communicate with the school and other adults accompanying the group on the outing.
- If pupils bring a mobile phone into the school this needs to be handed to the school secretary at the beginning of the day for safekeeping and collected at the end of the school day.
- The iPad is a school tool designed to enhance classroom practice. Children are not permitted to download or access any materials which is illegal, inappropriate or may cause harm or distress to others.
- If staff or pupils discover an unsuitable Apps on the IPad, it must be reported to the E-Safety Subject Leader, who will inform the network manager.

**11. Published Content and the School Web Site**

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

**12. Publishing Pupils' Images and Work**

- On a pupil's entry to the school, parents/carers will be asked to give permission for their child's photos to be used in a variety of ways. The purpose will be clearly explained and agreed including Learning Journeys, display and on some occasions other children's Learning Journeys. Parents must give specific consent for photographs to be used in newspapers, magazines etc. This consent will be considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.
- Parents/carers may withdraw permission, in writing, at any time.
- Pupils' full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Permission from parents or carers will be obtained before photographs of pupils are published.
- The school will request that any photos/images taken by parents during whole school events, such as concerts and sports day, will be for their personal use only and not be published on the internet including social networking sites.

**13. Information System Security**

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The information system security covers fixed and mobile Internet; school PCs, laptops, iPads and digital video equipment. It should also be noted that devices owned personally by staff and pupils but brought onto school premises (such as mobile phones, iPads, tablets, Kindles) are subject to the same requirements as technology provided by the school.

**14. Protecting Personal Data**

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Teachers may carry data on memory sticks or other removable data carriers in order to access their files both at home and at school. Any data carried in this way must be encrypted using appropriate encryption software, e.g. TrueCrypt.

**15. Assessing Risks**

- The school will take all reasonable precautions to prevent access to inappropriate material.
- The Network Manager will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

**16. 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.
- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

**17. Communication of Policy**

**17.1 Pupils**

- Rules for Internet access will be posted in classrooms, on the mobile unit and in the library.
- Pupils will be informed that Internet use will be monitored.
- As the pupils progress through the school, children will be taught these **SMART** tips (from Childnet International – www.childnet.com):
-

**S**afe – Keep safe by being careful not to give out personal information – such as your full name, e-mail address, phone number, home address, photos or school name – to people you are chatting with online.

**M**eeting – Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

**A**ccepting – Accepting e-mails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

**R**eliable – Information you find on the Internet may not be true, or someone online may be lying about who they are.

**T**ell – Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

You can report online abuse to the police at www.thinkuknow.co.uk

**17.2 Staff**

- All staff will be given the school E-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

**17.3 Parents**

- Parents' attention will be drawn to the school E-Safety Policy in newsletters and on the school web site.
- Parents will be informed about the SMART rules taught to the children in school and will be informed that they may wish to invest in security software for their own computers.
- 10 safety rules will be shared with parents (taken from the e-safety white paper):
  - maintain a basic understanding of computers
  - understand the digital safety issues that children face
  - monitor tools and programmes that children are using online
  - restrict how much time children are spending online,
  - communicate and be vigilant
  - establish ground rules to keep children safe online
  - apply usage policies and guidelines for social media
  - utilize resources to help protect children online
  - set ground rules for mobile technology
  - help children to understand e-safety.

**Monitoring and Review**

The E-Safety Policy will be reviewed annually by the E-Safety Subject Leader.

APPENDIX 1) E-Safety Rules 2) Think then Click 3) Respecting and caring for the whole-school community when taking photos and video 4) Staff Acceptable ICT User Agreement 5) Guide to the Use of Images

**March 2016 – Review March 2017**

**Key Stage 1**

# Think then Click

## These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

B. Stoneham & J. Barrett

**Key Stage 2**

# Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only e-mail people a teacher has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We do not open e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

# E-Safety Rules

These e-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any unauthorised person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

# Staff Acceptable ICT Use Agreement

**To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.**

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional rôle.
- I understand that school information systems may not be used for private purposes, without specific permission from the headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate authorised person.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-safety coordinator or the designated child protection coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

**I have read, understood and agree with the Information Systems Code of Conduct.**

Signed: ……

Capitals: ……..

Date: ……..

## Stanborough Primary School

# Respecting and Caring for the Whole School Community when taking Photos and Video

**We are happy for parents and carers to take photos and video of the school production for personal use on condition that these images are not distributed or put online. This is to protect all members of the school community**

CLICK CLEVER CLICK SAFE

Thank you for your support

Hertfordshire

# Stanborough Primary and Nursery School

# Guide to the use of

# Images

## Respecting and Caring for the Whole School Community

## Using Images Safely and Responsibly

We all enjoy and treasure images of our family and friends. Our new born baby, first steps, family events, holidays and school events are moments we all like to capture in photos or on video.

We then have the added and exciting dimension of adding our images and video to our social network, such as Facebook, YouTube and many other online websites. This means that we can easily share our photos and video with family and friends.

Whilst this is naturally useful, in schools and educational settings we do need to protect and safeguard all children and staff in our school, including those who do not want to have their images stored online.

## Online Images and Video

What should we think about before adding online any images or video? Are there any risks?

**Facts**

- Once online any image or video can be copied and stay online forever.
- Some children are at risk and MUST NOT have their image put online. Not all members of the school community will know who they are.
- Some people do not want their images online for personal or religious reasons.
- Some children and staff may have a complex family background which means that image sharing online can have unforeseen consequences.

We must all **'Think Before We Post' Online**

**At Stanborough Primary and Nursery School we are happy for parents and carers to take photos and video of the school production for personal use on condition that these images are not distributed or put online. This is to protect all members of the school community**

Thank you for your support

Further Information on the Use of Images and video can be found:

☺ **Be Safe Online**
http://tinyurl.com/ye24kxe

☺ **Information Commissioner's Office**
http://tinyurl.com/yc7nmnv

☺ **ThinkUknow**
http://www.thinkuknow.co.uk/parents/safeuse/

Developed by the
Hertfordshire Schools' eSafety Team