Southcote Primary School
E-Safety Policy

E-Safety encompasses the Internet and other electronic tools such as tablets, mobile phones and wifi. It is important to educate children and young people about both the benefits and risks of using this technology in order to provide safeguards and awareness for users to enable them to control their online experiences.

Good Habits

E-Safety depends on effective practice:

- Responsible ICT use by all staff and pupils; encouraged by education and supported by policies
- Sound implementation of the e-safety policy in both administration and curriculum, including secure school network design and use
- Safe and secure broadband from a supplier approved by Reading Borough Council network including the effective management of content filtering
- National Education Network standards and specifications

e-Safety Coordinator

- The e-Safety Coordinator is the Headteacher. In her absence, any Designated Safeguarding Officer fulfills this role.

Why is Internet Use Important?

- The Internet is used in school to raise educational standards, to promote pupil achievement and to enhance learnings within the National Curriculum
- Its use supports the professional work of staff and enhances the school management information and administration systems
- The school has a duty to provide pupils with quality Internet access as part of their learning experience because it is an essential element in modern life for education, business and social interaction
- Internet use is a part of the statutory curriculum. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use

- The Internet is a necessary tool for staff and pupils
- Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security

Internet use will enhance learning
(Appendix 1)

- Internet access within school includes filtering appropriate to the age of pupils
- Pupils will be taught about acceptable Internet use and will be given clear objectives
- Teachers carefully plan all Internet-based teaching to ensure that pupils are focused and using appropriate and relevant materials
- 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 knowledge location, retrieval and evaluation when using the Internet for research purposes
- Pupils are taught how to use search engines and how to evaluate Internet-based information as part of the Computing curriculum, and in other curriculum areas where necessary
- Pupils are taught how to recognise differences between commercial and non-commercial websites, and how to investigate the possible authors of web-based materials
- Pupils are taught how to carry out simple checks for bias and misinformation
- Pupils are taught that web-based resources have a similar copyright status as printed and recorded materials such as books, films and music, and that this must be taken into consideration when using them

Information System Security

- School ICT system capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly

Email

- Pupils are not allowed to access personal e-mail using school Internet facilities
- Forwarding of chain letters is not permitted
- If when using email, an offensive e-mail is received, pupils must inform the teacher immediately
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Members of staff should only use their school e-mail address for contact with pupils, parents or governors on school related matters
- E-mails sent to external organisations should be written carefully and with

consideration to the reputation of the school
- Staff are not allowed to use school IT equipment for personal use without prior approval from the Head

Downloading files and images

Pupils are not allowed to download any material from the Internet unless directed to do so by an appropriate staff member

Social Networking and Personal Publishing

- Schools should 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 and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils
- Staff are expected to model appropriate ICT and Internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils both in school and at home
- The school has a Social Media Policy for all members of staff which is reviewed and has been approved by the Governing Body

Personal use of the Internet and ICT resources

- Some equipment is available for loan to staff. The appropriate forms and agreements must be signed before items are taken away from the school
- Staff must be aware of the school policy about personal use of the equipment

Published Content and the School Web Site

- Contact details on the school website will be the school name, address, e-mail and telephone number
- Information about staff or governors will comply with statutory requirements

Publishing Pupils' Images and Work

- On admission to the school, parents/carers will be asked to consent to their child's photograph being published on the school website or other social media where appropriate
- Photographs that include pupils will be carefully selected
- Pupils' full names will not be used anywhere on the school website in association with photographs

Managing Filtering

- The school will work in partnership with the Local Authority, DfES and the IT Service Provider to ensure systems to protect pupils are reviewed and improved
- If anyone discovers unsuitable sites, the URL (address), time, content must be reported to the e- safety coordinator. Action will then be taken to ensure that access to this site is blocked
- Designated members of staff will ensure that regular checks are made to ensure the filtering methods selected are appropriate, effective and reasonable
- The school actively promotes the use of the Child Exploitation and Online Protection Centre (CEOP)

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- Pupils are not encouraged to bring a mobile phone or other electronic devices to school
- All pupils who require a mobile phone in order to walk to and from school must switch them off and hand them in to the school office for safe storage on arrival at school

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998
- Requests for data should be put in writing to the Headteacher
- The Headteacher will liaise with the Reading Borough Council Data Controller where necessary

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material
- However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access

- The school will audit ICT provision to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate

Mobile Phones

- The school has a separate Mobile Phone policy for all members of staff. This is reviewed regularly and has been approved by the Governing Body

Communication of the e-safety policy

- E-Safety rules will be posted in all classrooms and discussed with pupils at the start of each year (appendix 2)
- Pupils will be informed that network and Internet use will be monitored
- The school will arrange an e-safety day as appropriate, offering age appropriate information and tasks to pupils across the school
- All staff will read the e-Safety Policy and its importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Parents' attention will be drawn to the school e-Safety Policy in newsletters, on the school website and via the school e-safety parent workshops and resources
- Parents will be encouraged to use parental controls on home devices accessed by their children.
- Parents will be encouraged to closely monitor the use of internet devices, including games consoles and to have an awareness of the age ratings of Social Media, apps and games

Signed	L Telling Executive Headteacher
Date	Summer 2016
Ratified by Governors	Summer 2016
Review Date	Summer 2017

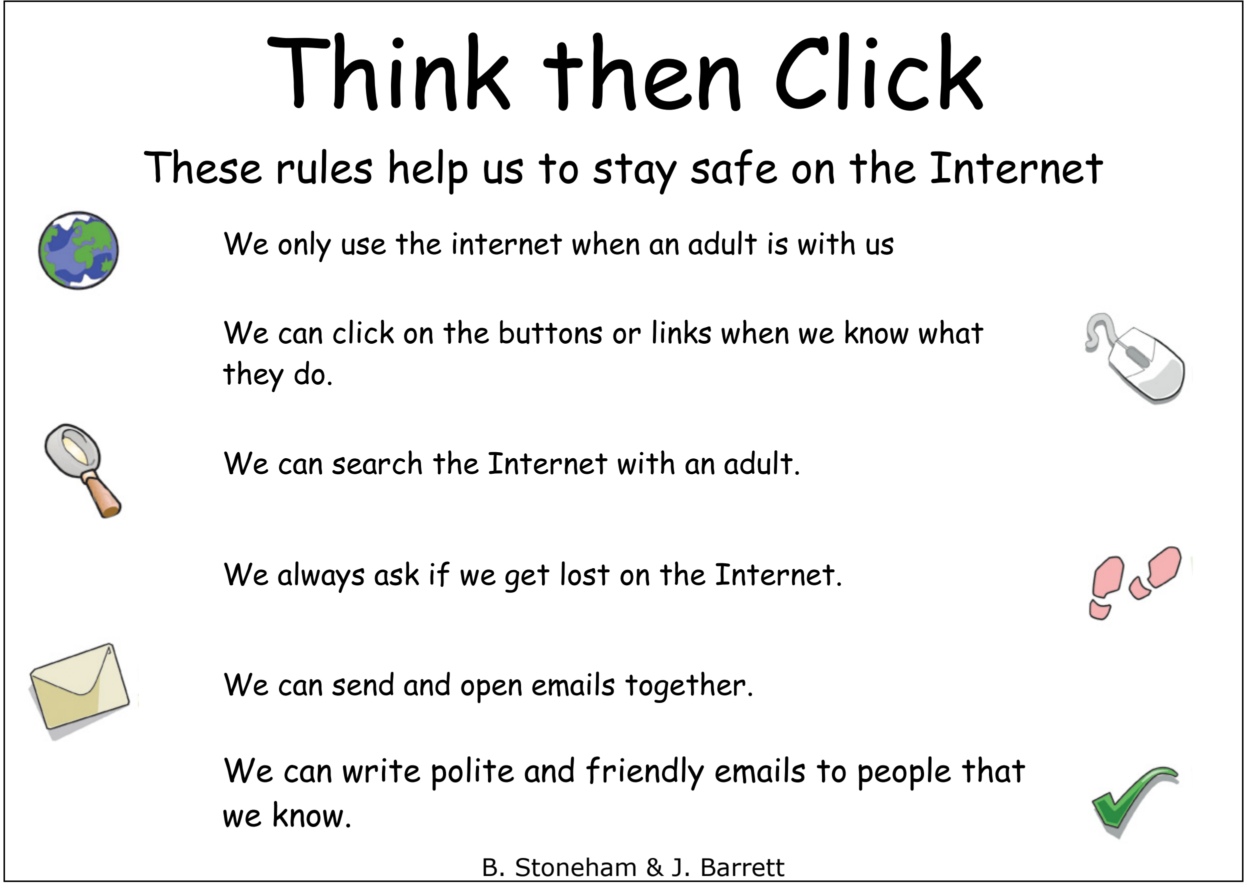
Appendix 1: Internet use - Possible teaching and learning activities

Activities	**Key e-safety issues**	**Relevant websites**
Creating web directories to provide easy access to suitable websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK South East Grid for Learning
Using search engines to access information from a range of websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Web quests e.g. - Ask Jeeves for kids - Yahooligans - CBBC Search - Kidsclick - Google (with high security settings)
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs.	Secure Learning Platform email. SuperClubs PLUS Gold Star Café School Net Global Kids Safe Mail E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	CC4g.net Making the News SuperClubs Infomapper Headline History Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked.	SuperClubs Skype FlashMeeting CC4G.net

	Pupils should never give out personal information.	
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype FlashMeeting National Archives "On-Line" Global Leap Natural History Museum

Appendix 2

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 not sure about.
- We only e-mail people an adult has approved.
- We send e-mails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails sent by anyone we don’t know.
- We do not use Internet chat rooms.