St Andrew's CE Primary School
E-Safety Policy – managing risks for children

Context

Internet use is part of the statutory curriculum and a necessary tool for learning. The National Curriculum (2014) requires that children:

- Use technology safely and respectfully.
- Know how to get help with and support for concerns about content or contact.

For further details of Computing curriculum expectations at each key stage see:
www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study

Children and staff rely on swift and easy access to the internet for a wide range of valid and valuable purposes; its 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. Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

There are potential dangers posed by use of the internet and other digital resources; this policy is written to explain how we manage these risks for children within the broader context of Child Protection and Safeguarding. The school will take all reasonable precautions to ensure that children access only appropriate material. However, due to the global and connected nature of content available via the Internet, it is not possible to guarantee that access to unsuitable material will never occur when using a school computer. Neither the school nor the local authority can accept liability for the material accessed, or any consequences resulting from Internet use. The use of school computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Any complaint about staff misuse must be referred to the head teacher. The school is aware that abuse can take place on digital platforms, such as social networking apps and websites, especially where there is open access without password protection allowing anyone to view the content. The school will be sensitive to online related issues experienced by pupils both in and out of school and offer appropriate advice and guidance.

Our e-Safety Policy has been written by the e-Safety coordinator, with advice and guidance from the Schools ICT dept. at Brighton and Hove City Council, e-Safety organisations and central government. It should be read in conjunction with other school policies available on http://www.st-andrews.brighton-hove.sch.uk/school-policies .

- Child Protection and Safeguarding Policy
- Teaching and Learning Policy
- Anti-bullying Policy
- Behaviour Policy
- Photographic & Video Images Policy
- Social Networking Policy

The school's designated person for Child Protection is Sarah Chambers and the e-Safety Coordinator is Carol Noble. Mr Cristin is the registered Data Protection Officer who is responsible for data security at the school.

This policy has been agreed by the senior management team and approved by the school's governing body. The e-Safety Policy and its implementation will be reviewed annually.

Expectations of staff

- e-Safety and digital awareness are taught as part of the Computing National Curriculum (2014). This covers instruction in responsible and safe use preceding Internet access and includes reasons for caution posting on digital platforms. Staff will guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity and ensure that pupils are aware that their network and Internet use will be monitored, as for all their other school work.

- At Key Stage 1, access to the Internet will be predominantly by adult demonstration with some directly supervised access to specific, teacher approved online materials. By the end of KS1 children should be taught how to '*use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies*'. (NC 2014)

- At Key Stage 2, access to the Internet will be by adult demonstration and increasing supervised direction to age appropriate online materials. By the end of KS2 children should be taught to '*understand computer networks including the internet… use search technologies effectively … use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.*' (NC 2014)

- All staff are given the School e-Safety Policy. Staff training in safe and responsible use of digital platforms will be provided as required.

- Staff are aware that Internet access by anyone at school can be monitored and traced to the individual user. It is essential that teachers exercise their professional discretion and conduct in line with their contract of employment. Teachers are advised not to run social network spaces for pupil use on a personal basis.

- Any material found on the school network and associated devices that the school believes is illegal may be reported to appropriate agencies such as the Child Exploitation & Online Protection Centre (http://www.ceop.police.uk) or the Internet Watch Foundation (https://www.iwf.org.uk) .

- The school currently filters Internet access using Smoothwall, which is maintained by the local authority. Senior staff will ensure that the filtering methods are regularly checked to be appropriate, effective and reasonable.

- If staff or pupils discover unsuitable websites via the school network, the URL must be reported to the e-Safety Coordinator or a senior manager to ensure that the filtering systems are updated. Children are taught to minimise rather than close such sites that they might discover to aid in this process.

- Digital communications sent by pupils to external organisations will be prepared carefully and authorised by a teacher, before sending, in the same way as a letter written on school headed paper. Unnamed examples of children's computing work may be published on areas of websites approved by senior management such as www.padlet.com.

- Pupils' full names will not be published online e.g. on the school's website, VLE or websites such as www.padlet.com. Written permission from parents or carers will be obtained before images of pupils are electronically published by the school. This is carried out as part of the admissions process.

Expectations of Children

Digital platforms accessed via the Internet are available for all pupils providing they show a responsible and mature approach to their use. Children who consistently demonstrate a positive attitude and aptitude for Computing will be nominated as Digital Leaders in their class. Purposeful misuse of digital platforms will be dealt with on a case by case basis by senior staff and may include sanctions within the school behaviour policy.

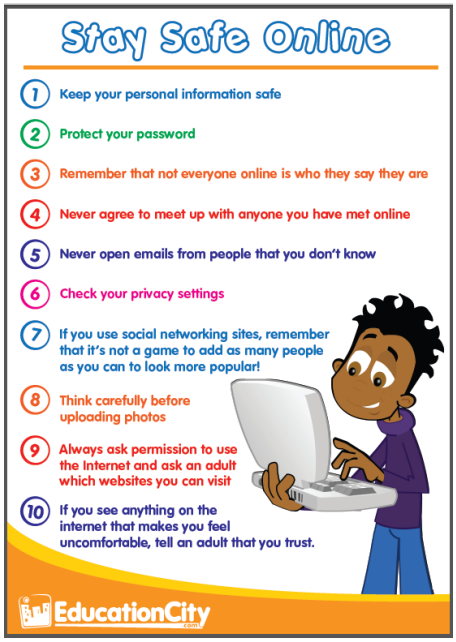
Children will learn to:

- Protect their personal information and keep it private, not share it with strangers and to ask a trusted adult if not sure.
- Be kind online. Tell a trusted adult if anyone is being mean online.
- Use Internet enabled devices as instructed by school staff. Hand in their own devices (e.g. phones, tablets etc.) to the school office on arrival.
- Immediately minimise or hide from view anything online that worries or concerns them and tell a teacher.
- Meet online friends with a trusted adult.
- Ask for permission to use copyrighted materials.
- Check the accuracy and authenticity of online content.

e-Safety posters are displayed by all fixed devices with Internet access in classrooms and the computer suite and should be referred to for guidance. For example;

For KS1

For KS2



Parental Support

A partnership approach with parents and carers is encouraged in all areas of school life. As part of e-Safety this could include parent evenings with demonstrations, suggestions for safe home Internet use posted on the school website and focus weeks at school.

Parents are asked to read the school's e-Safety Policy and are invited to ask for clarification or advice on any of the points; The best piece of advice from all agencies is for parents **to share and be aware** of their child's online activities, much as you would in any other public space.

Parents are asked to sign and return a consent form for pupil Internet access as part of the admissions process.

Parents and carers are asked to work in partnership with school staff to resolve issues of e-Safety so that they may be handled sensitively. However, parents need to be aware that in rare serious cases discussions may be held with the local Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

e-Safety References

This is not an exhaustive list but contains websites that offer advice to parents and some which have child centred activities that may be used in school.

Brighton and Hove Child Safeguarding	*www.brightonandhovelscb.org.uk*
CBBC Stay Safe	*www.bbc.co.uk/cbbc/topics/stay-safe*
Child Exploitation and Online Protection	*www.ceop.police.uk*
Child Net	*www.childnet.com*
Childline	*www.childline.org.uk*
Digital Awareness UK	*www.digitalawarenessuk.com*
Digizen	*www.digizen.org*
Internet Watch Foundation	*www.iwf.org.uk*
NAACE – National association for technology in education	*www.naace.co.uk*
National Education Network	*www.nen.gov.uk*
NSPCC / Netaware	*www.nspcc.org.uk* , *www.net-aware.org.uk*
Parent Zone – Digital Parenting Magazine	*parentzone.org.uk* , *parentinfo.org*
Safety Net	*www.safetynetkids.org.uk* , *www.safety-net.org.uk*
Think U Know (produced by CEOP)	*www.thinkuknow.co.uk*
Virtual Global Taskforce	*www.virtualglobaltaskforce.com*

Written by Carol Noble, Computing and e-Safety Curriculum Co-ordinator, June 2017

Next review date June 2018