Eastchurch Church of England Primary School

Internet Access and online safety Policy

Review Annually Next Review June 2018)

We at Eastchurch Primary School understand the important role that the Internet can provide when making sure our children receive a high-quality education. We live in a developing technological world where technology is taking a pivotal role. The internet is used in a variety of ways to promote teaching and learning. However, it is important that all members of staff and children at Eastchurch Primary are aware of the issues relating to Online Safety and Internet Access as outlined in the policy.

Our Internet Access and Online Safety Policy has been written by building on the KCC Online safety policy and government guidance. It has been agreed by the Senior Leadership team and approved by governors. All teaching and support staff have received a copy of the policy and signed to acknowledge this. It will be reviewed annually. This policy should be read alongside the school's Anti Bullying policy, Internet usage agreement and Safeguarding policy.

The importance of Internet use.

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 information and business administration systems. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

The Computing Curriculum (2014) outlines that pupils at Key Stage 1 should be taught 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.

The Computing Curriculum (2014) outlines that pupils at Key Stage 2 should be taught to:

- use search technologies effectively, appreciate how results are selected and ranked, and be discerning in evaluating digital content
- select, use and combine a variety of software (including internet services) on a range of digital devices to design and create a range of programs, systems and content that accomplish given goals, including collecting, analysing, evaluating and presenting data and information
- use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries
- inclusion in government initiatives such as the NGfL and the Virtual Teacher Centre (VTC)
- cultural, vocational, social and leisure use in libraries and clubs.
- staff professional development through access to national developments, educational materials and good curriculum practice exchange of curriculum and administration data with the LA and DfE.

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils using Lightspeed's Web filtering system, monitored by EIS and the school. The school will work with the LA, DFE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. We also monitor the filtering system to ensure we collect evidence of any blocked websites that have been attempted to be accessed.

Pupils will be taught what is acceptable and what is not acceptable and given clear objectives for Internet use. All classes will have regular lessons on e-safety throughout the Computing curriculum and will take part in the annual Internet safety day.

Useful e–Safety programs include:
• Think U Know: www.thinkuknow.co.uk
• Childnet: www.childnet.com
• Kidsmart: www.kidsmart.org.uk
• Orange Education: www1.orange.co.uk/education
• Safe: www.safesocialnetworking.org

At each site there are two Online Safety Ambassadors who have received training on online safety; they ensure that messages from the Internet safety Day are continually considered throughout the year. They also monitor, in collaboration with staff, the Online Safety Concern boxes. Children are able to post in any concerns they have had when using the internet or things they would like to know.

Rules for Internet access and online safety will be posted near all computer systems. These will be discussed with the children. In addition all children will be active members in suggesting their own ideas for a safer internet.

Internet access will be planned to enrich and extend learning activities. No children will access the Internet without suitable adult supervision. Parent's attention will be drawn to the School Online Safety Policy in the school prospectus and on the school Web site.

All staff will be given the School Internet Access and Online Safety Policy and its importance explained. All teaching and support staff will be asked to sign to acknowledge they understand the importance of Online safety. All staff who have access to the school computers sign an 'Acceptable ICT Use Code of Conduct'.

Pupils will be informed that Internet use will be monitored. Instruction in responsible and safe use should precede Internet access.

Evaluating Internet content
If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Subject Leader.
Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law. Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing e-mail.

- Pupils may only use approved e-mail accounts on the school system.
- Whole-class or group e-mail addresses should be used for all pupils unless they require an individual one for correspondence. They will be supervised while using them.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

Managing Website content.

- The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. Close up pictures of individual children should be avoided wherever possible. It may also be inappropriate to use images of pupils doing PE.
- Pupils' full names will not be used anywhere on the website when associated with photographs although it is, in normal conditions, possible to give the first names of pupils as this should not give away any information that could be harmful.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. (see Appendix 2)
- The Heads of School or nominee will take overall editorial responsibility and ensure content is accurate and appropriate (see Appendix 2).

Authorised Internet access.

- The school will keep a record of all staff and pupils who are granted Internet access.
- At Key Stage 1, access to the Internet will be by staff demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2 a teacher or other member of staff will grant the use of the Internet to a whole class or group as part of the curriculum area being covered.

Risk assessment.

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Methods to identify, assess and minimise risks will be reviewed regularly. Neither the school nor KCC can accept liability for the material accessed, or any consequences of Internet access.

Maintaining ICT system security.

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed and reviewed regularly.
- Files held on the school's network will be regularly checked.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- If staff or pupils discover an unsuitable site, it must be reported to the ICT/Online Safety Coordinator.

Social networking, social media and personal publishing

- The school will block access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Children will not enter chat rooms or social networking sites such as Facebook or Twitter.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils, please refer to our Social Media Policy.
- Staff wishing to use Social Media tools (Youtube) 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.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when

concerning students' underage use of sites.

Video conferencing

- All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

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 Heads of School.
- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying and behaviour.

The Heads of School will ensure that the Internet and Online Safety policy is implemented and compliance with the policy monitored.

The designated Online Safety governor is: …….

The School Online Safety Coordinators are ……

Policy approved by Head Teacher: …… Date: ……..

Policy approved by Governing Body: ……(Chair of Governors) Date: ……

The date for the next policy review is **June 2018**.

Appendix 1: Internet use – Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
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
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.	RM Easymail E-mail a children's author E-mail Museums and galleries
Publishing pupils' work on school and other websites.	Parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	School website Talk2Learn Kent Grid for Learning
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.	School website Talk2Learn Kent Grid for Learning BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderate should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	SuperClubs Flash Meeting

Appendix 2 – Consent Form

Dear Parent/Carer

During your child's schooling at Eastchurch Primary school, there will be many activities and events that your child will participate in that we do need consent for.

Please read through the list below and indicate if your consent is given for the following by ***deleting as appropriate*** and signing.

Child's name _____

***I do / *I do not** give consent for my child to participate in **school outings and field trips around the village** and to a member of staff acting on my behalf in the event of an emergency.

Signed _____ Parent/Carer

***I do / *I do not** give consent for my child to take part in any **group** photographs that maybe used on our **school website**.
(We do not use photographs of individual children on our school website and no names are printed)

Signed _____ Parent/Carer

***I do / * I do not** give consent for my child's photograph and first name to be published in our **local paper**. (children's full names are not published unless appropriate to the picture, if this is the case you will be contacted for permission by telephone on the day)

Signed _____Parent/Guardian

***I do / *I do not** give consent for my child to be videoed by the school during school activities.

Signed _____Parent/Carer

This form will be kept on your child's record through out their schooling at Eastchurch School.