Caversham Primary School

eSafety Policy

Policy reviewed and updated: November 2016

Next policy review: November 2017

Review check-list:

Date of latest update (at least annual): *November 2016*	
The school eSafety policy was agreed by governors on: *06.11.14*	
The policy is available for staff: *school network at the following location:* *Staff Common / Admin / POLICIES SEPT 12 ONWARDS / Curriculum / latest policies*	
The policy is available for parents/carers at: *School Office*	
The responsible member of the Senior Leadership Team is: *Russell Wood (Middle Leadership)*	
The responsible member of the Governing Body is: *Anthony Morris*	
The Designated Child Protection Coordinator is: *Ruth Perry*	
The eSafety Coordinator is: *Russell Wood (Computing Leader)*	
Has eSafety training been provided for both pupils and staff?	**Y**
Is there a clear procedure for a response to an incident of concern?	**Y**
Have eSafety materials from CEOP and Becta been obtained?	**Y**
Do all staff sign a Code of Conduct for ICT on appointment?	**Y**
Are all pupils aware of the eSafety rules?	**Y**
Are eSafety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	**Y**
Do parents/carers sign and return an agreement that their child will comply with the school eSafety rules?	**Y**
Are staff, pupils, parents/carers and visitors aware that network and internet use is closely monitored and individual usage can be traced?	**Y**
Has an ICT security audit been initiated by SLT, possibly using external expertise?	**Y**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y**
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements?	**Y**
Has the school-level filtering been designed to reflect educational objectives and approved by SLT?	**Y**

Caversham Primary School

eSafety Policy

Date of Policy: November 2016 Review Date: November 2017

eSafety encompasses internet technologies and electronic communications such as mobile phones, video and audio recorders. 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.

2.1 Writing and reviewing the eSafety policy:

- The eSafety policy relates to other policies including ICT acceptable use policies, the bullying policy and the school policy for child protection.
- The school has an appointed eSafety coordinator. This is Russell Wood as he is also the Computing leader and a member of the MLT.
- Our eSafety Policy has been written by the school. It has been agreed by senior management and approved by governors and the PTA.
- The eSafety Policy and its implementation will be reviewed annually.
- The eSafety Policy was revised by: Russell Wood
- The original version was approved by the Governors on: 06.11.2014

2.2 Teaching and learning

2.2.1 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.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

2.2.2 How will internet use enhance learning?

- The school internet access is two-fold. Pupils have their own user names and passwords under which they have access to the internet that has been tailored to include an appropriate filtering system. The filtering system is monitored by the school and computing provider Soft Egg. Staff have their own usernames and can access the internet without it being filtered in order that they may select appropriate

learning resources from otherwise limited sites e.g. YouTube. Staff have been trained to ensure children cannot see content from unrestricted sites before they have been vetted by teaching staff.

- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use.
- 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 shown how to publish and present information to a wider audience safely.

2.2.3 Pupils will be taught how to evaluate internet content:

- Pupils should 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, offensive or suspicious internet content in school and their private lives.

2.3 Managing Internet Access

2.3.1 Information system security:

- School ICT system's capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the school's computing provider.

2.3.2 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.
- The forwarding of chain letters is not permitted.
- Pupils must not open e-mails from people that they do not know or attachments that are from an unknown source.

2.3.3 Published content and the school website:

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

2.3.4 Publishing pupil images and work:

- Pupils' full names will not be used anywhere on the website.
- Written permission is given by parents and carers as children enter the school for photographs of pupils to be published on the school website. Only images of children that have this clearance will be used.

- Photographs that include pupils will be selected carefully so that the image cannot be misused.
- Requests to parents and children to publish their work on the website will be made on an individual basis. Work can only be published with signed permission.

2.3.5 Social networking and personal publishing:

- The school will block access to social networking sites for all pupils.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils will be taught the importance of not placing personal photos on any social network space.
- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and to block unwanted communications.
- Pupils will be advised to use nicknames/avatars when using social networking sites.
- Parents and pupils will be made aware of the dangers of using social networking sites.
- The school will advise any child they know to be using social networking sites with age restrictions that they are in breach of the rules of the site. The school will inform the child's parents of their inappropriate use.

2.3.6 Managing filtering:

- The school will work in partnership with the LA, DfES and the internet service provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the eSafety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

2.3.8 Managing emerging technologies:

- Emerging technologies will be examined for educational benefit and staff will discuss the risks of this equipment before use in school is permitted.
- The school mobile phone must only be used by staff members and for school purposes.
- Digital cameras and video recorders will be used with close supervision by staff. These items will be stored safely so that they are not accessible without a member of staff.
- All staff and pupils will be trained to use the VLE appropriately. The administrator will monitor use.
- Gaming is strictly prohibited unless special compensation is given by a member of staff who has checked that the gaming sites are appropriate prior to use.

2.3.9 Protecting personal data:

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

2.4 Policy Decisions

2.4.1 Authorising internet access:

- All staff must read and sign the Acceptable Use Policy for Staff before using any school ICT resource. This includes part-time and peripatetic staff. Any person not directly employed by the school will be asked to sign an acceptable use agreement before being granted access to the internet from school.
- Temporary visitors to the school may use the network, and should seek the Computing Leader or ICT Technician for access details (username and password)
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.

2.4.2 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 should audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate at each review date.
- Memory sticks must be checked for viruses/infections by the ICT Technician before being plugged into a computer attached to the school network

2.4.3 Handling eSafety complaints:

- Complaints of internet misuse will be dealt with by a senior member of staff and logged alongside bullying incidents. Records will be kept in the school office.
- 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.

- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of the consequences for pupils misusing the internet.

2.5 Communications Policy

2.5.1 Introducing the eSafety policy to pupils:

- ESafety rules will be posted in all rooms and on the desktop of each pupil user. These will be discussed regularly.
- Pupils will be informed that network and internet use will be monitored and misuse followed up.
- A programme of training in eSafety will be developed based on materials from CEOP.
- ESafety talks will be embedded in the ICT scheme of work.
- All pupils from Year 3-6 will sign an acceptable use policy and parental permission will be obtained for them to access the internet.

2.5.2 Staff and the eSafety policy:

- All staff will be given the school eSafety 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.
- All changes to filtering will be supervised by SLT.
- All staff will always explore internet searches and programmes thoroughly to check that they are appropriate before using them with pupils.

2.5.3 Enlisting parents' support:

- Parents' attention will be drawn to the school eSafety policy in newsletters, the school brochure and on the school website.
- The school will maintain a list of eSafety resources for parents/carers.
- The school will ask all new parents to sign the pupil/parent agreement when they register their child with the school.
- Annual talks in eSafety will be provided for the parents prior to their children receiving an eSafety talk.

Appendix 1: Useful Resources for Parents

Think you know:	http://www.thinkuknow.co.uk
Child Exploitation and Online Protection:	http://www.ceop.gov.uk/
Microsoft online safety:	http://www.microsoft.com/protect/
Care for the family:	www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
Childnet International "Know It All" CD:	http://publications.teachernet.gov.uk
Family Online Safe Institute:	www.fosi.org

Appendix 2: Useful Resources for Teachers

BBC Stay Safe:	www.bbc.co.uk/cbbc/help/safesurfing/
Becta:	http://schools.becta.org.uk/index.php?section=is
Chat Danger:	www.chatdanger.com/
Child Exploitation and Online Protection:	www.ceop.gov.uk/
Childnet:	www.childnet-int.org/
Cyber Café:	http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx
Digizen:	www.digizen.org/
Kent eSafety materials:	www.clusterweb.org.uk/kcn/eSafety_home.cfm
Kidsmart:	www.kidsmart.org.uk/
Think U Know:	www.thinkuknow.co.uk/
Safer Children in the Digital World:	www.dfes.gov.uk/byronreview/