ST. PETER'S CHURCH OF ENGLAND (VC) PRIMARY SCHOOL

E-SAFETY POLICY

ONLINE SAFETY

Who has written the policy and who has verified it?

Our school internet policy has been created by Miss Foster (E-safety Lead) in consultation with Mr. Unthank, Mrs. Marsay, and Mr. David Major using information from BECTa, Redcar and Cleveland Local Authority and government guidance. This policy has been developed since 2011. It has been discussed by the whole staff and approved by governors who realise how intrinsic to the running of the school, both at a management level and an educational level, the internet is. The policy has been reviewed by Miss Foster in November 2016 and discussed with Governors. The policy will be reviewed September 2017.

Why have this policy?

The internet is now the most data rich source of information in the world. It can potentially "bring the world into the classroom." From a teaching point of view this is an essential resource for planning and delivering lessons. From a child's point of view it is an excellent source of information that enhances the personalised learning agenda.

The internet based school learning platform allows effective dissemination of specific information (notes, dates, files) to specific people (teachers, parents, staff). This will be a place to upload files that they have created and access appropriate resources. Increasingly the internet is becoming a place to share information, collaborate with others and our school would like utilise the learning platform to enhance the education of all children. Essentially this will be integral to most ways of working in the workplaces that they will eventually enter.

This policy seeks to ensure users know what good practice is and outlines steps and procedures that will be taken when the darker side of the internet shows itself.

Name	Title	Signature	Date
Richard Unthank	Headteacher	R.P. Unthank	02/02/17
Miranda Foster	E-Safety Leader	M. Foster	02/02/17
Neil Selley	Health & Safety Nominated Governor		02/02/17
June Marsay	Assistant Head	J A Marsay	02/02/17

Filtering

The school's broadband connection is provided by Claranet via their ADSL Max Broadband Network and can provide speeds up to 20mbps. The School is protected by a comprehensive industry standard firewall and Internet filter. The Internet Filter (Webwall) filters the Internet on a number of fronts:

- Lists of questionable sites which are blocked,
- Custom designed active contend filtering based on key words.

Net 3 provide our ICT support an in the occurrence of a problem we would contact them in the first instance.

If a member of staff came across an unsuitable website they would need to switch the monitor off to prevent children from seeing the website and contact Miss M Foster or Mr. Unthank who would then contact Net 3 to allow them to look into the website to have it blocked.

However, when dealing with the internet there is never a failsafe way of blocking inappropriate content in all situations and therefore the school cannot take responsibility for these events when all reasonable steps outlined above have been taken. In addition to this is the consideration that children will inevitably access the internet outside of school. We therefore aim to educate them about internet safety, not simply cover their eyes.

When will pupils have direct access to the internet?

All staff with network accounts and children in all classes in school will have access to the internet. This is in the form of a personal login account on the network, or through using a tablet device.

Children will not be allowed to access and search the internet unless **authorised by a member of staff.** In this respect, children will be monitored, however it is not possible to oversee each child use each device (iPod/Kindle) to use the internet. So the following rules are put into place:

- The only search the item they were told to
- They access the website they were told to
- If they come across a problem, they are to press the home button and notify a member of staff immediately

Accessing and interacting with the internet is part and parcel of many users' reasons for having an internet connection. Simply blocking the children from using internet it is not educating them for the real world (and use at home). Therefore internet safety is implicitly taught to pupils and referred to whenever a unit of work requires use of the internet (first in Autumn term 2012). Key themes to be covered are listed below:

- Safe browsing on the internet
- Use of chatrooms
- Use of blogs/webspace
- Use of email
- What to do when you come across something that is inappropriate

Staff have found the following websites to be a valuable source of teaching materials and resources:

www.Thinkuknow.co.uk

childnet.com

ceop.police.uk

kidsmart.org.uk

saferinternet.org

In accordance with the Data Protection Act 1984/98, users are not allowed to access other user's personal files and folders. The exception to this being system administrators who can gain access through permission from the Headteacher when just cause has been established.

How can the children manage their own files?

Children have their own workspace online through ***mydesktop***. They will be given this after agreeing to the terms and conditions in the home/school agreement. The children will use their space for storing files and organising information. Inappropriate materials or text found on ***mydesktop*** will result in being reported to the Headteacher, and possibly the child having their account terminated. The children will be taught how to use this space to create a portfolio of their work and links to/copies of resources that they use to complete their school work. Personal files should be stored elsewhere. Administrators reserve the right to access personal ***mydesktop*** space when requested by the Headteacher.

From September 2014, all children from Year 3 onwards to Year 6 will need to create their own personal login for the network. This can be done by pressing ***control+alt+delete*** which then asks you to ***'change password'***. The children will be asked to create a case sensitive password with a number and to not share it with others. The teacher will collate the passwords in case the child forgets but their accounts will not be accessed by staff other than to help support the child.

Children's use of mobile devices.

Mobile phones are not permitted to be used within school unless permission has been granted by the Headteacher . Failure to observe this will result in confiscation. School staff can confiscate a mobile phone as a disciplinary penalty, and have a legal defence in respect to this in the Education and Inspections Act 2006 (s94). Staff cannot search the contents of a pupil's mobile phone without the consent of that pupil. Where a pupil refuses to allow the contents of his/her phone to be searched, the matter can be referred to the police who have more extensive search powers.

Children will have access to iPod and iPad devices in school under the supervision of staff who will instruct which ***applications*** would be used to complete the set task. Children will have a responsibility to use the iPod and iPad in the manner which they have been asked to do so. The iPod and iPad have access to the internet via Wi-Fi set up and maintained by Net3. Any issues need to be brought to the attention of Miss Foster or Mr. Unthank who will contact Net3.

Children may take mobile phones and tablets/hand held devices on residential visits if they have been granted permission by the Headteacher and their parents. The school is not liable for them during this time. Children shall be asked to hand in their switched off devices and mobile phones whilst they are in their rooms on an evening and will be given them back when appropriate.

Communication.

How should the children manage their email?

If pupils are granted an email account, they may only use approved email accounts that have been given to them from school and only when they are instructed to by staff. Ig introduced then this shall only be for children from Year 4 onwards when the children shall be given an ***Outlook 365*** account like the staff. These accounts are not to be used as personal email account. Pupils must not send inappropriate emails and should never disclose their personal information to others such as their address or telephone number. When using their school emails to write to an external organisation they should be written in the same careful manner and authorised before sending, just like the children would if they were sending a letter on the school's headed paper.

Children's use of online communications and social networking.

Pupils will be taught how to keep personal information safe when using online services. Each year group shall receive age-specific lessons dedicated to E-safety. The school will conduct informal annual pupil surveys about home use of IT. This will support teachers when choosing a range of activities which pupils undertake and how safely they are using them, e.g. how to keep themselves safe on sites etc. The use of online chat is not permitted in school, other than it being part of an online learning environment. Any child found to be communicating through online chatrooms or messaging services will be spoken to, and the website will be locked. The Headteacher will be informed and parents will be contacted if necessary.

The Child Protection Advisor for St Peter's, is invited on an annual basis to work with the children on E-Safety. Parents are also given the opportunity to attend workshops with to develop their knowledge and understanding on how to manage and monitor their child's internet activity.

How will this policy be introduced to Children?

This will be done through the consent booklet when the child first joins the school (see Appendix 1 – Rules for Responsible Internet Use). Internet use guides should be placed around school to be discussed with children in Foundation Stage and KS1, and for KS2 children to read. Teachers should go through this policy with their children at a level that they understand, and to be repeated as frequently as necessary.

How should this policy be introduced to Parents?

A copy of this policy will be on the School Website. References to E-Safety will be mentioned in letters to Parents' on a basis that is applicable and handled in a sensitive manner. Internet issues can be discussed with; the Headteacher; the School Learning Mentor or the child's class teacher at a parent's discretion, should the need arise.

How should this policy be introduced to Staff?

A copy of this policy will be on the School Website and in the staff handbook and the staff will receive regular online training. All staff must accept this policy and the Acceptable Use Policy before accessing the network or wireless internet in school.

How will complaints be handled?

In the first instance of this policy being contravened, the child will be reminded as to what should be done (i.e. if someone goes on a website they shouldn't). If a more severe issue occurs, then the parents shall be contacted by a member of senior staff if deemed more appropriate than the class teacher. If a parent feels that this is inappropriate they should contact the Headteacher or the Complaints Committee of the Governing Body.

DECLARATION

I accept the terms and conditions outlined within this E-Safety Policy.

Signed: .....

Role: .....

Date: .....

Appendix 1

St. Peter's Church of England (VC) Primary School

Rules for Responsible Internet Use

For their own protection the pupils at St. Peter's School have limited access to the Internet through the schools Intranet system. The following rules will keep everyone safe and help us to be fair to others:

- I will only access the system with my own user name.
- I will not access other pupils' files.
- I will only open and delete my files, or those that my teacher has told me to access.
- I will only use the computers for schoolwork and homework.
- I will not bring memory sticks or CD ROMs from outside school, unless I have been given permission by a member of staff.
- I will ask permission from a member of staff before using the Internet as part of teaching and learning programmes.
- I will only e-mail people my teacher has approved.
- I will only download files, pictures and images after permission is given by my teacher.
- The messages I send will be polite and responsible.
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent or teacher has given permission.
- I understand that the school checks my computer files and monitors the sites I visit.
- If I see anything I am unhappy with, or I receive messages I do not like, I will tell a teacher immediately.
- I understand that if I do not follow these rules that I may not be allowed to use the Internet, computers or mobile devices within school.

Name of pupil: .....

Signed by pupil: .....

Signed by parent: .....

Date: .....

Appendix 2:

Keeping Children Safe in Education September 2016

Online safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene in and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- content: being exposed to illegal, inappropriate or harmful material;
- contact: being subjected to harmful online interaction with other users; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Filters and monitoring

Governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with a safe environment in which to learn, governing bodies and proprietors should consider the age range of their pupils, the number of pupils, how often they access the IT system and the proportionality of costs vs risks.

The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part by the risk assessment required by the Prevent Duty.

The UK Safer Internet Centre has published guidance as to what "appropriate" might look like:
- UK Safer Internet Centre: appropriate filtering and monitoring

Guidance on e-security is available from the National Education Network-NEN. Buying advice for schools is available here: buying for schools.
Whilst filtering and monitoring are an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school approach to online safety. This will include a clear policy on the use of mobile technology in the school. Many children have unlimited and unrestricted access to the internet via 3G and 4G in particular and the school and college should carefully consider how this is managed on their premises.

Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 64) and the requirement to ensure children are taught about safeguarding, including online (paragraph 68), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Information and support

There is a wealth of information available to support schools and colleges to keep children safe online. The following is not exhaustive but should provide a useful starting point:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation