Park Street Church of England eSafety Policy

Approved at FGB

5th February 2015

Contents

This policy has been written in working with children, staff and parents of Park Street Church of England Primary School. It is an adaptation and personalisation of a model policy drafted by the Kent County Council eSafety Policy and government guidance. It has been agreed by the Senior Leadership Team and approved by governors and the PTA.

Section 1 - Teaching and learning eSafety

a) Why is Internet use important?

- Internet use is part of the statutory curriculum and an important tool for learning.
- The school has a duty to provide students with quality Internet access as part of their learning experience.
- The Internet is a part of everyday life for education, business and social interaction.
- Pupils use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.
- 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 functions.

b) How does Internet use benefit education?

The benefits of using the Internet in education include:

- access to worldwide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils worldwide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across networks of schools, support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data
- access to learning wherever and whenever convenient.

c) How can Internet use enhance learning?

- The school's Internet access will be designed to enhance and extend education.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

- The schools will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and maturity.
- 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 taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

d) How will pupils learn how to evaluate Internet content?

- Pupils at KS2 will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- When being taught how to research internet content, age-appropriate controls will be in place and age-appropriate guidance given.

Section 2 - Managing the School's Information Systems

a) How will information systems security be maintained?

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be kept up to date.
- Personal data sent over the internet or taken off site will be encrypted, where possible.
- The use of logins and passwords to access the school system will be enforced.

b) How will email be managed?

- Pupils will only use Starz email accounts.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult.
- Whole class or group email addresses will be used in primary schools for communication outside of the school.
- Staff should only use school email accounts to communicate with pupils as approved by the Senior Leadership Team.
- Staff should not use personal email accounts during school hours (excluding non directed / lunchtime / after school) or for professional purposes

c) How will published content be managed?

- The contact details on the website should be the school address, email and telephone number. Staff or pupils' personal information must not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website will comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

d) Can pupil's images or work be published?

- Images that include pupils will be selected carefully.
- Pupils' names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before images of pupils are electronically published.
- Pupils' work can only be published with the permission of their parents. (Appendix C – Parents Consent Form)

e) How will social networking, social media and personal publishing be managed?

- The school controls access to social media and social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location and / or their status. 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, age, gender, etc.
- Pupils will be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Attention should be given regarding background detail in a photograph which could identify the student or his/her location.
- Staff official blogs or wikis should be password protected and run from the school website with approval from the Senior Leadership Team. Staff are not permitted to run social network spaces for pupil use on a personal basis.
- If personal publishing is to be used with pupils, then it must be via age-appropriate sites suitable for educational purposes with the prior approval of the Senior Leadership Team. Personal information must not be published and the site must be moderated by school staff.
- All members of the school community are advised of the importance of security and encouraged to set passwords, deny access to unknown individuals and instructed on how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others by making profiles private. (Appendix F)
- Pupils are advised not to publish specific and detailed private thoughts,

especially those that may be considered threatening, hurtful or defamatory.

- Staff personal use of social networking, social media and personal publishing sites (as discussed as part of staff induction), and safe and professional behaviour is outlined in the school's Acceptable Use Policy (Appendix A).
- Parents are strongly advised not to publish any images or commentary of other people's children on any social media or publishing platform because there may be unknown risk factors in so doing, no matter how innocent it may seem.

f) How will filtering be managed?

- Park Street Church of England Primary School uses the county-provided filtering service, which ensures that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL must be reported to the e–Safety Coordinator. (Appendix D – eSafety incident reporting form)
- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- Any material suspected to be illegal will be reported by the school to appropriate agencies such as Internet Watch Foundation (IWF) or Child Exploitation and Online Protection Centre (CEOP).
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the pupils, with advice from the County's ICT Service.

g) How are emerging technologies managed?

- Staff will be issued with a school phone where contact with pupils is required.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- Emerging technologies will be considered on a case-by-case basis, depending on the perceived educational benefit and risk for the school.

h) How should personal data be protected?

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

Section 3 - Policy Decision-making in Practice

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the School Acceptable Use Policy and the Safer Code of Conduct Policy before using any school ICT resource. (Appendix A – Acceptable Use Policy)
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with supervised Internet access. (Appendix C)

a) How will risks be assessed?

- The school takes all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.
- The school's Leadership Team monitors the e–Safety policy to ensure it is adequate and that its implementation is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

b) How will the school respond to any incidents of concern?

- Where there is cause for concern or fear that illegal activity has taken place or is taking place involving the use of computer equipment, the Leadership Team will determine the level of response necessary for the offence disclosed.
- All members of the school community will be kept informed of eSafety concerns (such as breaches of filtering, cyberbullying, illegal content etc).
- The Designated Child Protection Coordinator will be informed of any eSafety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage eSafety incidents in accordance with the school discipline/behaviour policy where appropriate.
- The school will inform parents/carers of any incidents of concerns as and when required.
- After any investigations are completed, the school will debrief, indentify lessons learnt and implement any changes required.
- Where there is cause for concern or fear that illegal activity has taken place or is taking place, then the school will contact the Children's Safeguard Team and escalate the concern to the Police

c) How will eSafety complaints be handled?

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- Any complaint about staff misuse must be referred to the headteacher.
- All eSafety complaints and incidents will be recorded by the school — including any actions taken.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will work in partnership with staff to resolve issues.
- Where deemed appropriate, discussions will be held with the local Police Safer Schools Partnership Coordinators and/or Children's Safeguarding Unit to establish procedures for handling potentially illegal issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

d) How is the Internet used across the community?

- Where beneficial to the school in the view of the Leadership Team, the school will liaise with local organisations improve eSafety at the school.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

e) How will Cyberbullying be managed?

- Cyberbullying (along with all forms of bullying) is not tolerated in the school. Full details are set out in the school's policy on anti-bullying.
- There are clear procedures in place to support anyone affected by Cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- Incidents or allegations of Cyberbullying will be responded to in accordance with the anti-bullying policy.
- Pupils, staff and parents/carers are advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in Cyberbullying may include:
    - The bully will be asked to remove any material deemed to be inappropriate or offensive.
    - A service provider may be contacted to remove content.
    - Internet access may be suspended at school for the user for a period of time.
    - Parent/carers will be informed.

- The Police will be contacted if a criminal offence is suspected.

f) How will Learning Platforms and learning environments be managed?

- Staff will monitor the usage of the LP by pupils and staff regularly in all areas, in particular message and communication tools and publishing facilities.
- Pupils/staff will be advised on acceptable conduct and use when using the learning platform.
- Only members of the current pupil, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, pupils etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.
- Any concerns with content may be recorded and dealt with in the following ways:

  a) The user will be asked to remove any material deemed to be inappropriate or offensive.

  b) The material will be removed by the site administrator if the user does not comply.

  c) Access to the LP for the user may be suspended.

  d) The user will need to discuss the issues with a member of SLT before reinstatement.

  e) A pupil's parent/carer may be informed.
- Pupils may require editorial approval from a member of staff. This may be given to the pupil to fulfil a specific aim and may have a limited time frame.

g) How will mobile phones and personal devices be managed?

- Pupils in Class 4 may bring a mobile phone to school. These must be placed in the school office during the school day.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor does the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

Pupils Use of Personal Devices

- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.

Staff Use of Personal Devices

- Staff will be issued with a school phone where contact with pupils or parents/carers is required.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by the Headteacher in emergency circumstances.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Section 4 - Communication of the eSafety Policy

a) How will the policy be introduced to pupils?

- All users will be informed that network and Internet use will be monitored.
- Pupil instruction in responsible and safe use should precede Internet access. (Appendix B – Key Stage 1 & 2 Rules, Appendix C – Parental permission Appendix E – Suggested Websites for eSafety Training)
- An eSafety module will be included in Computing Curriculum each year covering both safe school and home use.
- Safe and responsible use of the internet and technology will be reinforced across the curriculum. Particular attention will be given where pupils are considered to be vulnerable.

b) How will the policy be discussed with staff?

- The eSafety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement the Acceptable Use Policy (Appendix A).
- Staff will be made aware that Internet traffic is monitored and can be traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use both professionally and personally will be provided.

c) How will parents' support be encouraged?

- Parents' attention will be drawn to the School eSafety Policy in newsletters, the school brochure and on the school website.
- A partnership approach with parents will be encouraged. This could include parent evenings with demonstrations and suggestions for safe home Internet use or highlighting eSafety at other attended events e.g. parent evenings,

sports days.

- Parents will be requested to sign an eSafety/internet agreement as part of the Home School Agreement.
- Information and guidance for parents on eSafety will be made available to parents in a variety of formats.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Section 5 - Useful eSafety Contacts and References

Becta: *www.becta.org.uk/safeguarding*

CEOP (Child Exploitation and Online Protection Centre*): www.ceop.police.uk*

CFE e–Safety Officer, KCC Children Families & Education
Rebecca Avery email: esafetyofficer@kent.gov.uk Tel: 01622 221469

Childline: *www.childline.org.uk*

Childnet: *www.childnet.com*

Children's Officer for Training & Development, Child Protection
Mike O'Connell email: mike.oconnell@kent.gov.uk Tel: 01622 696677

Children's Safeguards Service: *www.kenttrustweb.org.uk?safeguards*

Click Clever Click Safe Campaign: *http://clickcleverclicksafe.direct.gov.uk*

Cybermentors: *www.cybermentors.org.uk*

Digizen: *www.digizen.org.uk*

E**IS - ICT Support for Schools and ICT Security Advice:**
www.eiskent.co.uk?ictsecurity

Internet Watch Foundation: *www.iwf.org.uk*

Kent e–Safety in Schools Guidance: *www.kenttrustweb.org.uk?esafety* (Includes a Schools Audit Tool and Notes on the Legal Framework as part of the PDF versions of this document)

Kent Primary Advisory e–Safety Pages:
www.kenttrustweb.org.uk/kentict/kentict_home.cfm

Kent Public Service Network (KPSN): *www.kpsn.net*

Kent Safeguarding Children Board (KSCB): *www.kscb.org.uk*

Kidsmart: *www.kidsmart.org.uk*

Schools Broadband Team - Help with filtering and network security:
www.eiskent.co.uk Tel: 01622 206040

Schools e–Safety Blog: *www.kenttrustweb.org.uk?esafetyblog*

Teach Today: *http://en.teachtoday.eu*

Think U Know website: *www.thinkuknow.co.uk*

Virtual Global Taskforce — Report Abuse: *www.virtualglobaltaskforce.com*

Appendix A: Staff Acceptable Use Policy

I agree and accept that any computer or laptop given or loaned to me by the school is provided solely to support my professional responsibilities. I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's management information system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority. I understand that all Internet usage / and network usage is logged and tracked and this information could be made available to my manager on request.

I will

- only use the school's digital technology resources and systems for professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- use the approved, secure email system(s) for all school business with pupils or parents/carers and only communicate with them on appropriate school business.
- ensure all documents, data etc. are saved, accessed and deleted in accordance with the school's network and data security and confidentiality protocols.
- report any accidental access to, or receipt of inappropriate materials, or filtering breach to the eSafety Coordinator, Designated Person for Child Protection or Headteacher, as appropriate
- use the school's Learning Platform in accordance with school and Local Authority advice.
- ensure that any private social networking sites / blogs etc that I create, or to which I contribute, do not compromise and are not confused with my professional role.
- ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- promote eSafety with pupils in my care and will help them to develop a responsible attitude to their use of ICT.

I will not

- share or reveal password(s) to anyone.
- allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- engage in any online activity that may compromise my professional responsibilities
- allow children to logon using my username and password

- browse, download or send material that could be considered offensive, illegal or discriminatory.
- download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- connect a computer, laptop or other device (including USB flash drive), to the network / Internet that does not have up-to-date anti-virus software.
- use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and
- I will not store images of pupils or staff at home or off-site without permission.

I understand that once I sign this document, failure to comply with this agreement could lead to disciplinary action.

Signed_____

Date_____

Appendix B: Park Street Schools e-Safety Rules and Agreement

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. The following is taken from Appendix B of our e-Safety Policy. You can view our full e-safety policy on the school website or ask for a copy from the school office.

Think Then Click

These rules help us to stay safe on the Internet

e-Safety Rules for Reception and Key Stage One

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.

e-Safety Rules for KS2

These rules help us to be fair to others and keep everyone safe.

I will ask permission before using the internet.

I will use only my class network login.

I will only open or delete my own files.

I understand that I must not bring into school and use software or files without permission.

I will only e-mail and open attachments from people I know, or my teacher has approved.

The messages I send will be polite and sensible.

I understand that I must never give my home address or phone number, or arrange to meet someone.

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 the school may check my computer files, e-mails I send and the internet sites I visit.

I understand that if I deliberately break these rules, I may not be allowed to use the internet or computers.

I will never post photographs or video clips of people I know without permission and never include names with photographs or videos.

Appendix C: Parent's Consent Form

Dear Parents/Carers

As part of the school's information and communications technology (ICT) programme, we offer pupils supervised access to the internet and email. Before the school allows students to use these facilities, they must obtain parental permission. Both pupils and parents must sign and return an Internet Use Permission Form as evidence of their acceptance of the school's rules for responsible ICT use.

Various projects have proved the educational benefits of internet and email access, which enable pupils to explore a wide range of information sources and communicate and collaborate with other learners throughout the world. Although there are concerns about children having access to inappropriate material via the internet, the school takes a range of measures to minimise these risks. A filtering system is in operation which restricts access to inappropriate materials and this is supplemented by an internet safety programme for all pupils, which teaches the safe and appropriate behaviours to adopt when using the internet, email and other technologies. Teachers will supervise and guide pupils towards appropriate material.

Although internet use is supervised and filtered within the school, families should be aware that some pupils may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive. As with any other area, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources at home. The school therefore supports and respects each family's right to decide whether or not to apply for access.

If you decide to support your child's application for access to the internet, please complete and return to the school office the form on the back of this letter as soon as possible.

Yours sincerely,

Mrs Gillian Owen

Internet and email use permission form

Please complete the form, including pupil's name and your signature and name, and return it to the school office

PUPIL'S NAME:

I understand that the school has rules concerning the use of the internet and agree to comply with them. I will use the internet, email and other ICT facilities at school in a safe and responsible way and will observe all the restrictions explained to me by the school.

SIGNATURE: **DATE:**

PARENT'S NAME:

As the legal guardian of the child named above I give permission for him/her to use the internet and other ICT facilities at school.

I understand that the school will take reasonable precautions to ensure that pupils cannot access inappropriate materials, including the teaching of internet safety skills to pupils, but accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the internet.

I accept responsibility for setting and conveying standards for my child to follow when selecting, sharing and exploring information and media and acknowledge that my child will be deemed responsible for his or her own actions.

□

OR

I refuse permission for the child named above to use the internet. □

SIGNATURE: **DATE:**

Appendix D: eSafety Incident Reporting Form

Date of incident:	
Member of staff reporting incident:	
Url, (web address) of incident:	
Copy of screens/evidence saved to:	
Location of incident (room):	
Computer number if known:	
Details:	
Passed to:	
Action taken	

Appendix E: Suggested websites for eSafety teaching

- Think U Know: ***www.thinkuknow.co.uk***
- Childnet: ***www.childnet.com***

Appendix F: Guidelines for staff using Social Networking sites.

Social networks are very popular and used by all ages in society. The most popular social networks are web-based, commercial, and not designed for educational use. They include sites like Facebook, Twitter, LinkedIn, Google Plus and many more. For individuals, social networking sites provide tremendous potential opportunities for staying in touch with friends and family.

As childcare workers we have a professional image to uphold and how we conduct ourselves online helps determine this image. As reported by the media, there have been instances of childcare professionals demonstrating professional misconduct while engaging in inappropriate dialogue about their setting and/or children, staff and parents; or posting pictures and videos of themselves engaged in inappropriate activity. Increasingly, staffs' online identities are too often public and can cause serious repercussions, both privately and professionally.

One of the hallmarks of social networks is the ability to "friend" or "connect with" or "follow" others – creating a group of others that share interests and personal news. **You are advised not to accept invitations to *friend* children and/or parents within these social networking sites**. When children and parents gain access into a worker's network of friends and acquaintances and are able to view personal photos, the dynamic is altered. 'Friending' children and parents provide more information than one should share in an educational setting. It is important to maintain a professional relationship to avoid relationships that could misconstrued; and/or are contrary to the the Guidance for Safer Working Practices for Adults who Work with Children and Young People

For the protection of your professional reputation, it is expected that you comply with the following practices:

Friends and friending

- Do not initiate friendships with children
- Remember that people classified as "friends" have the ability to download and share your information with others.

Content

- Do not write or respond to anything deemed to be defamatory, obscene, proprietary, or libellous.
- Exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations.
- Weigh whether a particular posting puts your effectiveness as a childcare professional at risk.

- Post only what you want the world to see. Imagine that all work contacts are all able visit the site. It is not like posting something to your web site or blog and then realising that a story or photo should be taken down. On a social networking site, basically once you post something it is likely to be available, even after it is removed from the site.
- Do not discuss children, parents or co-workers or publicly criticise the school's policies, activities or staff.
- Do not post images that include children and/or parents.

Security

- Visit your profile's security and privacy settings. At a minimum, childcare professionals should have all privacy settings set to "only friends", and security settings should be set high to avoid the potential for hacking of your accounts.
- You are advised against having your privacy settings set to include unknown people, for example "Friends of friends" on Facebook, because this opens your content to a large group of unknown people. Opening your content to unknown people will put your privacy, that of your family, and anyone about whom you communicate at risk.

Aide Memoire for School Leadership: Action Checklist

- Virus protection will be monitored (2b)
- Maintain current record of all staff and pupils with access to school's electronic communications (3)
- All staff must read and sign the School Acceptable Use Policy and the Safer Code of Conduct Policy before using any school ICT resource (3)
- Parents will be asked to sign and return a consent form for pupil access (3)
- Parents will be informed that pupils will be provided with supervised Internet access (3)
- A Designated Child Protection Co-ordinator required to be informed of eSafety incidents (3b)
- Establish procedures to support anyone affected by cyber-bullying (3e)
- Ensure when staff, pupils, etc leave school that their access is removed / disabled (3f)
- Provide a copy of the eSafety policy to all staff (4b)
- Ensure that staff who manage filtering systems are monitored by the Leadership Team a propos this responsibility (4b)