St Peter in Thanet Church of England Junior School

e-safety Policy

The policy

- The school has appointed an e–Safety Coordinator.
- The e–Safety Policy and its implementation will be reviewed annually.
- Our e–Safety Policy has been written by the school, building on the KCC e–Safety Policy and government guidance.

The School e-Safety Coordinator is Debbi Spurgin

Policy approved by Head Teacher & L&D Team 16.1.15

The date for the next policy review is October 2015

St Peter's Vision for the Use of ICT

The use of technology in the 21st century is a part of everyday life for education, business and social interaction. It is essential that we harness the power of these tools to ensure that St Peter's is a dynamic learning environment where we help pupils to enjoy and achieve. We acknowledge that with new technologies, such as the Internet, there are associated risks including accessing inappropriate content, receiving unwanted attention or being vulnerable to cyber bullying. At St Peter's we believe that everyone must be highly aware of the dangers related to the use of ICT and the measures that need to be taken in order to safely maximise the potential of ICT .

Teaching and learning

Why is Internet use important?

- Internet use is part of the statutory curriculum and is a necessary tool for learning.
- The Internet is a part of everyday 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.
- 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.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

How does Internet use benefit education?

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 with KCC and DfE;
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

Pupils need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught.

- 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 to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- Staff should guide pupils to online activities that will support the learning outcomes planned for the pupils' age and ability.
- 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.

How will pupils learn how to evaluate Internet content?

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will use age-appropriate tools to research Internet content.

Managing Information Systems

How will information systems security be maintained?

The Schools Broadband network is protected by a cluster of high performance firewalls at the Internet connecting nodes in Maidstone and Canterbury. These industry leading appliances are monitored and maintained by a specialist security command centre.

- St Peter's ICT system security is reviewed regularly.
- Virus protection is installed and updated regularly.
- Unapproved software will not be allowed in work areas or attached to email.
- Files held on the school's network will be regularly checked.
- The network manager will review system capacity regularly.

How will email be managed?

Email is an essential means of communication for both staff and pupils. Directed email use can bring significant educational benefits; interesting projects between schools in neighbouring villages and in different continents can be created, for example.

- Pupils may only use approved email accounts for school purposes.
- Pupils must immediately tell a designated member of staff 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 will only use official school provided email accounts to communicate with pupils and parents/carers, as approved by the Senior Leadership Team.

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.
- Images or videos that include pupils will be selected carefully and will not provide material that could be reused.
- Pupils' full 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/videos of pupils are electronically published.

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

Examples of social media and personal publishing tools include: blogs, wikis, social networking, forums, bulletin boards, multiplayer online gaming, chatrooms, instant messenger and many others.

- The school will control 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. 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.
- Staff wishing to use Social Media tools 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. Staff will obtain documented consent from the Senior Leadership Team before using Social Media tools in the classroom.
- 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.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy.
- Staff are instructed that when using social networking sites for personal use they must not contact or communicate with students or parents/carers.

How will filtering be managed?

It is important that children should always be supervised when using internet access and that Acceptable Use Policies are in place. In addition, Internet Safety Rules should be displayed, and both children and adults should be educated about the risks online.

There should also be an Incident Log to report breaches of filtering or inappropriate content being accessed. Procedures need to be established to report such incidents to parents and KCC (The Schools Broadband Service Desk at EiS or the e-Safety Officer) where appropriate.

Any material that the school believes is illegal must be reported to appropriate agencies such as IWF, Kent Police or CEOP.

Websites which schools believe should be blocked centrally should be reported to the Schools Broadband Service Desk. Teachers should always evaluate any websites/search engines before using them with their students; this includes websites shown in class as well as websites accessed directly by the pupils. Often this will mean checking the websites, search results etc just before the lesson. Remember that a site considered safe one day may be changed due to the Internet being a dynamic entity.

- The school's broadband access will include filtering appropriate to the age and maturity of pupils.
- The school will work with KCC and the Schools Broadband team to ensure that filtering policy is continually reviewed.
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all pupils) will be aware of this procedure.
- If staff or pupils discover unsuitable sites, the URL will be reported to the School e-Safety Coordinator who will then record the incident and escalate the concern as appropriate.
- The School filtering system will block all sites on the Internet Watch Foundation (IWF) list.

How will videoconferencing be managed?

Videoconferencing enables users to see and hear each other between different locations. The school may decide to use Facetime or Skype from time to time.

- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the students' age.
- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.

How are emerging technologies managed?

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access. This can offer immense opportunities for learning as well as dangers.

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The use by students of cameras in iPads or other devices is encouraged if it is for education purposes but is monitored by the teacher. Publishing or distribution of recorded information may only occur with the express permission by the teacher.
- Pupils will be instructed about safe and appropriate use of personal devices both on and off site in accordance with the school Acceptable Use.

How should personal data be protected?

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

The eight principles are that personal data must be:

- Processed fairly and lawfully
- Processed for specified purposes
- Adequate, relevant and not excessive
- Accurate and up-to-date
- Held no longer than is necessary
- Processed in line with individual's rights
- Kept secure
- Transferred only to other countries with suitable security measures.

How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff will read and sign the 'Staff Information Systems Code of Conduct' or School Acceptable Use Policy before using any school ICT resources.
- Parents will be asked to read the School Acceptable Use Policy for pupil access and discuss it with their child, where appropriate.
- Pupils will be supervised. Pupils will use age-appropriate search engines and online tools and online activities will be teacher-directed where necessary.

How will risks be assessed?

- The school will take 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. Neither the school nor KCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The school will audit ICT use to establish if the e–Safety policy is adequate and that the implementation of the e–Safety policy is appropriate.

How will the school respond to any incidents of concern?

- The e-Safety Coordinator will record all reported incidents and actions taken in the School e-Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.

- Serious incidents of a safeguarding nature will be dealt with in accordance with "Dealing with Incidents of Concern" procedure.
- The Designated Child Protection Coordinator will be informed of any e-Safety incidents involving Child Protection concerns, which will then be escalated appropriately.
- The school will manage e-Safety 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.

Communicating about e-Safety

Introducing the e-safety policy to pupils

- E-Safety rules which have been developed and designed by the pupils will be posted in rooms where computers are used.
- Pupils will be informed that network and Internet use will be monitored.
- A programme of training in e-Safety will be developed, possibly based on the materials from CEOP.

How will e–Safety complaints be handled?

- Complaints about Internet misuse will be dealt with under the School's complaints procedure.
- Any complaint about staff misuse will be referred to the head teacher.
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken.

How is the Internet used across the community?

- The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

How will Cyberbullying be managed?

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

- 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.
- There are clear procedures in place to support anyone in the school community affected by cyberbullying.
- All incidents of cyberbullying reported to the school will be recorded.
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying.

How will iPads and other personal devices be managed?

Mobile phones, iPads and other personal devices such as Games Consoles, Tablets, PDAs and MP3 Players etc. are considered to be an everyday item in today's society and even young children may own and use personal devices to get online regularly. Mobile phones, iPads and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

However, mobile devices can present a number of problems when not used appropriately:

1. They are valuable items which may be stolen or damaged;
2. Their use can render pupils or staff subject to cyberbullying;
3. Internet access on phones and personal devices can allow pupils to bypass school security settings and filtering;
4. Phones or IPads with integrated cameras could lead to child protection, bullying and data protection issues with regard to inappropriate capture, use or distribution of images of pupils or staff.

- The use of iPads by students and staff in school will be covered in the school Acceptable Use Policy.
- The sending of abusive or inappropriate messages or content via iPads or mobile devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school discipline/behaviour policy.
- School staff may confiscate a device if they believe it is being used to contravene the schools behaviour or bullying policy. The device might be searched by the Senior Leadership team .If there is suspicion that the material on the mobile device may provide evidence relating to a criminal offence the device will be handed over to the police for further investigation.
- IPads will be used during lessons or formal school time as part of an approved and directed curriculum based activity with consent from a member of staff.
- The Bluetooth function of an iPad should be switched off at all times and not be used to send images or files to other unless with consent from a member of staff.

5. The iPads are not permitted to be used in certain areas within the school such as toilets.

Pupils Use of Personal Devices

- If a pupil breaches the school policy then the iPad or other mobile 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.
- Students will be instructed in safe and appropriate use of iPads and personal devices and will be made aware of boundaries and consequences.

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.
- 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 a member of Senior Leadership Team 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.

How will the policy be introduced to pupils?

- All users will be informed that network and Internet use will be monitored.
- An e–Safety training programme will be established across the school to raise the awareness and importance of safe and responsible internet use amongst pupils.
- An e–Safety module will be included in the PSHE, Citizenship and/or ICT programmes covering both safe school and home use
- e-Safety rules or copies of the student Acceptable Use Policy will be posted in all rooms with Internet access.
- Safe and responsible use of the Internet and technology will be reinforced across the curriculum and subject areas.

Staff and the e-Safety policy

- The e–Safety Policy will be formally provided to and discussed with all members of staff.
- To protect all staff and pupils, the school will implement Acceptable Use Policies.
- Staff will be made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible Internet use, both professionally and personally, will be provided for all members of staff.

How will parents’ support be enlisted?

- Parents’ attention will be drawn to the school e–Safety Policy in newsletters, the school prospectus and on the school website.
- To help parents to understand more about iPads, the school will run courses and parent awareness sessions when handing out the devices.
- A partnership approach to e-Safety at home and at school with parents will be encouraged. This may include offering parent evenings with demonstrations and suggestions for safe home Internet use to coincide with Safer Internet Day.
- Parents will be requested to sign an e–Safety/Internet agreement as part of the Home School Agreement.
- Parents will be requested to sign an iPad agreement if taking part in our Home Access scheme .

- Parents will be encouraged to read the school Acceptable Use Policy for pupils and discuss it’s implications with their children.
- Information and guidance for parents on e–Safety will be made available to parents in a variety of formats including files on the iPad.
- Advice on useful resources and websites, filtering systems and educational and leisure activities which include responsible use of the Internet will be made available to parents.