St Peter's Catholic Primary School

e-Safety Policy

June 2018

This document has been produced in line with the issued guidance and associated materials as declared on the Wirral LA

eSafety Policy

The school has appointed Julie Farrelly as the eSafety co-ordinator.
David Colley assists the Head Teacher in this role.
Our eSafety Policy has been written by the school.
It has been agreed by the Senior Management Team.

The eSafety Policy will be reviewed annually. This policy will next be reviewed in **June 2018** .

Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality Internet access

Students will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient
- Access to world-wide educational resources including museums and art galleries
- Educational and cultural exchanges between students world-wide
- Access to experts in many fields for students and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across 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 the Local Authority and DCSF

How Can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for student use and includes filtering appropriate to the age of students
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide students in on-line activities that will support learning outcomes planned for the students' age and maturity
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

Authorised Internet Access

- The school will maintain a current record of all staff and students who are granted Internet access
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource
- Parents will be informed that students will be provided with supervised Internet access
- Parents will be asked to sign and return a consent form for student access
- Students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement

World Wide Web

- If staff or students discover unsuitable sites, the URL (address), time, content must be reported to the eSafety Co-ordinator and recorded in the eSafety log.
- School will ensure that the use of Internet derived materials by students and staff complies with copyright law
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy

VLE

- Students must sign an AUP explicitly for the VLE.
- Parents sign & return student consent form for VLE.

Email

- Students may only use approved messaging systems (eschools) on the school system
- Students must immediately tell a teacher if they receive offensive message (Report button)
- Students must not reveal personal details of themselves or others in messages communication, or arrange to meet anyone without specific permission
- Access in school to external personal e-mail accounts may be blocked
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain letters is not permitted

Password Protection

- School issues passwords.
- Staff & students encouraged to change their passwords on a regular basis.
- No use of generic passwords.
- Students must not disclose passwords to other students.

Social Networking

- The School will should block/filter access to social networking sites and newsgroups unless a specific use is approved.
- Students will be advised never to give out personal details of any kind which may identify them or their location
- Students should be advised not to place personal photos on any social network space. Photos placed on website/e-schools/ must be approved by Website administrators (consent will be checked before photo is added)
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others
- All staff/adults associated with the school have a responsibility to ensure professionalism at all times. Therefore, Facebook/Twitter accounts must be kept private at all times and kept up-to-date with the highest level of security settings. Status'/photos must also show that person in a positive light (staff code of conduct). Parents/pupils/ex pupils should not be accepted as friends unless they are a family member.

Filtering

The school will work in partnership with the Local Authority to ensure filtering systems are as effective as possible.

Video Conferencing

- Pupils should ask permission from the supervising teacher before making or answering a videoconference call
- Videoconferencing will be appropriately supervised for the pupils' age

USB memory sticks & other Portable Data Storage Devices

- All staff have an encrypted memory stick to ensure all school data is kept secure. Staff should not hold school data on any other devise unless agreed with the Headteacher.

Digital Cameras

- Staff to use school cameras to photograph students(Check consent forms)
- Staff must not use personal equipment to photograph students.
- Storage cards to be cleared when camera returned.

Storage of Photographs

- Photographs to be stored in secure area within school network.
- Photographs to remain on school premises (when practicable –i.e. off site school trips – images only to be downloaded to school network.

- Photographs to be deleted when no longer required.
- Current school policy is adhered to regarding photographing & publishing images of children

Mobile Phones & Other Hand Held/Communication devices

- Mobile phones & other hand held communication devices should not be used for personal use in the lesson or formal school time (students & staff).
- Mobile phones are not used in classrooms

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out by the safeguarding officer and agreed by the governing body, before use in school is allowed.
- Mobile phones/ handheld communications devices/ gaming consoles will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden

Published Content and the School Web Site

- The contact details on the Web site will be the school address, e-mail and telephone number. Staff or pupils personal information will not be published. Staff names will be published due to OFSTED website requirements.
- Website Administrators Stephen Gregson and Julie Farrelly will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Students' Images and Work

- Photographs that include students will be selected carefully and will be appropriate for the context
- Students' full names will not be used anywhere on the Web site, VLE or Blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site or VLE
- Work can only be published with the permission of the student and parents

Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly
- Security strategies will be discussed with the Local Authority
- Also see the use of 'USB memory sticks and other portable storage devices' section.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material including those which may radicalize pupils. 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. Neither the school nor Wirral Metropolitan Borough Council can accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the eSafety policy is adequate and that the implementation of the eSafety policy is appropriate every 12 months.

Handling eSafety Complaints

- Complaints of Internet misuse will be dealt with by Julie Farrelly, Safeguarding officer and Headteacher
- Any complaint about staff misuse must be referred to Headteacher.
- 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

Training

Students

PSHE/Outside agencies/embedded across the curriculum
Age appropriate

Staff

All staff (teaching & non teaching)
Outside agencies/LA
Yearly review of training
INSET

Governors

Outside agencies/LA
Yearly review of training

Parents

Sessions/workshops for parents

Communication of Policy

Students

- Rules for Internet access will be posted in the ICT classroom
- Students will be informed that Internet use will be monitored

Staff

- 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
- Staff that manage filtering systems or monitor ICT use will be supervised by Karen Sparks/Senior Management and have clear procedures for reporting issues

Governors

- AUP

Parents

- Parents' attention will be drawn to the School eSafety Policy in newsletters, the school brochure and on the school Web site

Visitors

- Visitors to school will be informed about the eSafety policy at the reception desk
- Rules for visitors clearly displayed (i.e. use of mobile phone/camera/film equipment/tablets etc).

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's eSafety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school eSafety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with students are compatible with my professional role.
- I will promote eSafety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.
- If applicable, I will keep my social networking accounts private and up-to-date with security settings, ensuring my professionalism is upheld (status'/photos) and that my friend list does not include parents/pupils/ex-pupils under any circumstances unless they are a family member.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. The school may also enforce capability procedures on anyone not adhering to the policy/code of conduct.

I have read, understood and agree with the Information Systems Code of Conduct.

Printed name: ……

Signed: …… Date:……..

St Peter's Catholic Primary School – Acceptable User Policy – Key Stage 2

eSafety Rules

All students use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both students and their parents/carers are asked to sign to show that the eSafety Rules have been understood and agreed.

Name:	***Class:***

Students' Agreement

- I have read and I understand the school eSafety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Child's Signature:	**Date:**

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published on the school VLE or The Life Channel within school. Yes ☐ No ☐

I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names. . Yes ☐ No ☐

Parent's Consent for Internet Access

I have read and understood the school eSafety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that students cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Parent's signature:	***Date:***

Please print name:

Please complete, sign and return to the school

Appendix A: KS 2 eSafety Rules

eSafety Rules

These eSafety Rules help to protect students and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Only use sites approved by a member of staff.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school will exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Appendix B: Key Stage 1 AUP Children

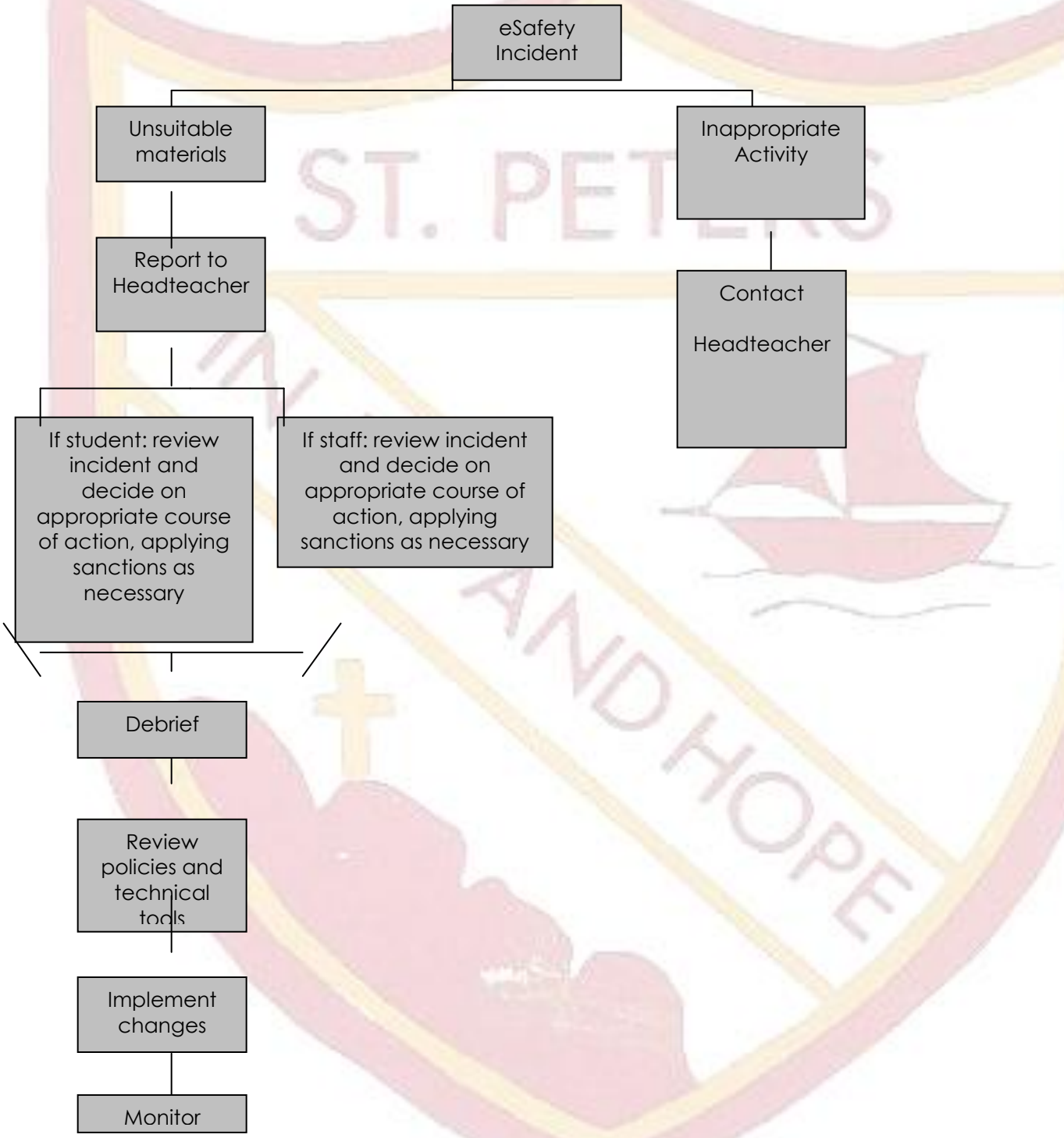
Think Before You Click

Use these rules to stay safe when using the Internet

S 	I will only use the Internet and email with an adult
A 	I will only click on icons and links when I know they are safe
F 	I will only send friendly and polite messages
E 	If I see something I don't like on the screen, I will always tell an adult

My Name
My Signature

Appendix C: Flowchart for responding to eSafety incidents



Appendix D: eSafety Audit

This quick self-audit will help the senior management team (SMT) assess whether the eSafety basics are in place.

Has the school an eSafety Policy that complies with CYPD guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The designated Child Protection Teacher/Officer is:	
The eSafety Coordinator is:	
Has eSafety training been provided for both students and staff?	Y/N
Is the Think U Know training being considered?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the School eSafety Rules?	Y/N
Have school eSafety Rules been set for students?	Y/N
Are these Rules displayed in all rooms with computers?	Y/N
Is Internet access provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access?	Y/N
Has the school filtering policy been approved by SMT?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of SMT?	Y/N

Appendix E: Are you an eSafe school?

Do all your staff...	Does your school...
☐ Understand e-safety issues and risks? ☐ Receive regular training and updates? ☐ Know how to escalate an issue of concern? ☐ Know how to keep data safe and secure? ☐ Know how to protect themselves online? ☐ Know how to conduct themselves professionally online? ☐ Know about the updated e-safety guidance for QTS standard Q21: Health and well-being?	☐ Have a nominated e-safety co-ordinator? ☐ Audit its e-safety measures? ☐ Have a robust AUP? ☐ Use a Becta accredited supplier for internet services? ☐ Include e-safety measures in Section 4b of your SEF? ☐ Keep an incident log and monitor your measures? ☐ Handle cyberbullying issues well? ☐ Raise awareness of the issues, E.g. through holding an assembly?
Do your learners...	**Do your parents and governors...**
☐ Understand what safe and responsible online behaviour means? ☐ Receive e-safety education at appropriate places across the curriculum? ☐ Get the opportunity to improve their digital literacy skills? ☐ Know the SMART rules? ☐ Know how to report any concerns they may have?	☐ Understand e-safety issues and risks? ☐ Understand their roles and responsibilities? ☐ Receive regular training and updates? ☐ Understand how to protect their children in the home?

Appendix F: Website log

Request to **unblock** a website to be used by Staff and/or Pupils for educational purposes.

Website Address	Reason	Staff	Date	Agreed Y/N	H/T Sig

Request to **block** a website.

Website Address	Reason	Staff	Date	Agreed Y/N	H/T Sig

Appendix G: eSafety Incident Log

Date	Staff	Incident	Action

St Peter's Catholic Primary School – Consent – Key Stage1

eSafety Rules

All students use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum.

Both students and their parents/carers are asked to sign to show that the eSafety Rules have been understood and agreed.

Name:	***Class:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published on the school VLE or The Life Channel within school. Yes ☐ No ☐

I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names. . Yes ☐ No ☐

Parent's Consent for Internet Access

I have read and understood the school eSafety rules and give permission for my son / daughter to access the Internet.

I understand that the school will take all reasonable precautions to ensure that students cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Parent's signature:	***Date:***

Please print name:

Please complete, sign and return to the school.