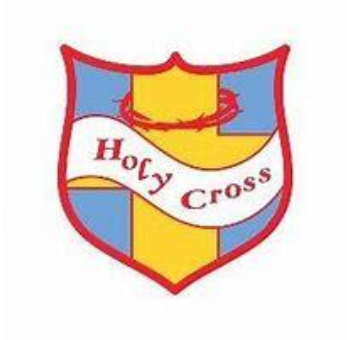
Holy Cross Catholic



Promoting E-Safety Policy

September 2020

Contents

Our E-safety policy

The school's e-Safety Coordinator is the head teacher; Mrs Clare Higgins. This policy is reviewed by the safeguarding team led by our Designated Safeguarding Lead (Mrs Clare Higgins) and our computing subject lead.

Introduction to E-Safety

1.1 E-Safety in a Changing World

At Holy Cross Catholic Primary School we celebrate the value and importance of technology in our children's learning. In our school; personal computers, wireless laptops, I-pads, digital voice recorders, camcorders and digital cameras are all part of children's every day learning. The internet has become a vital source of learning and communication for all members of our school community.

Pupils interact with new technologies such as mobile phones and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial but can occasionally place young people in danger.

Our school seeks to provide the right balance between controlling access, setting rules and educating students for responsible use. During the forthcoming year we are;

- Re-launching our school's website. Our school website has a host of materials to guide families on the use of ICT and E-Safety
- Revising how E-safety is taught as part of our PSHE and computing curriculum.
- Holding sessions for children and parents on E-Safety with school staff.
- Developed Digital Champions in KS2 (previously E-Cadets).

The term E-safety covers the issues relating to young people and their safe use of the Internet, mobile phones and other electronic communication technologies. This policy assesses the protocols for ensuring that these initiatives are carefully developed in our school, so that we progress responsibly and appropriately in the interests of our children. It also looks at how we educate our children to be safe in a world where technology is so readily available.

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible ICT and computing use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;

- Secure, filtered broadband that the school manages with our partners at EXA Internet filtering and our colleagues at Hi-Impact;
- A school network that complies with the National Education Network standards and specifications (we have maintained old BECTA standards).
- Effective school based training. E-safety is reviewed annually as part of our safeguarding training.

1.2 E-Safety and the Legal Issues

E-safety should be practised to protect children, staff and all members of our school community. Our School's e-Safety Policy replaces the Internet Policy to reflect the need to raise awareness of the safety issues associated with information systems and electronic communications as a whole.

Our E-safety commitments related to our safeguarding policy, anti-bullying policy and the school's Prevent Duty policy.

E-Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

Much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others.

Schools need to protect themselves from legal challenge. The law is catching up with Internet developments: for example it is a criminal offence to store images showing child abuse and to use email, text or Instant Messaging (IM) to 'groom' children. In addition there are many grey areas for schools to consider regarding communication of social network sites, storage of data etc.

Schools can help protect themselves by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised". However, schools should be aware that a disclaimer is not sufficient to

protect a school from a claim of personal injury and the school needs to ensure that all reasonable actions have been taken and measures put in place to protect users.

In practice this means that this school ensures that;

- It has effective firewalls and filters on our school network.
- Ensures that e-safety responsibilities are clearly communicated to all members of our school community.
- That our Acceptable Use Policies are fully enforced for children, staff and visitors. This includes supply teachers, volunteers and associate teachers.
- Ensures that our procedures are consistent with the Data Protection Act (1998)

Learning and Teaching in the Digital Age

The school uses wireless laptops and comprehensive broadband access to develop learning and teaching through digital communication. Access to instant messenger services and mobile phones is not allowed as part of this school's curriculum. However, the school will include provision to educate children how to use this technology appropriately and safely.

2.1 Why the Internet and digital communications are important

Mobile Communication equipment and the Internet are an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. We also recognise that children are actively engaged with digital communication form an early age. It is part of their lifelong learning experiences and habits. We also have a responsibility to ensure that our children learn to use these opportunities and resources responsibly, appropriately and productively to enhance their learning.

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

2.2 Encouraging responsible use of the Internet and digital communication.

1. The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. This is arranged through the school's needs with Wirral IT support. Only sites directly approved by the head teacher will be allowed to override the filter.

2. Pupils will be taught about responsible and appropriate information sharing through the internet and other forms of digital communication.

3. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

4. Pupils will be taught about responsible use of e-mails and other sources of digital communication including e-mail, messenger services and texts.

5. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

6. Pupils will be shown how to publish and present information to a wider audience safely and responsibly.

2.3 Pupils will be taught how to evaluate Internet and other digital communication content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils will be taught the importance of cross-checking information before accepting its accuracy.

- Pupils will be taught how to report unpleasant Internet or other digital content including messages, e-mails and texts. Whilst we cannot promote the use of social networking sites, we must also ensure that our children know how to manage the risks and dangers associated with these activities.

Managing Digital Access, Communication and Content

All Internet accessed is managed by the school. Individual users should only access the Internet through their username and password. The school recognises that password protection is vital element of promoting e-safety.

The school will ensure that permission for access and use of any content including photographs is fully explained and sought.

3.1 Information system security

- School ICT systems security will be reviewed regularly. This will be part of the liaison between the head teacher and our partners at Wirral IT services.
- Virus protection will be updated regularly as part of the school's Service Level Agreement with Wirral IT Services.
- Security strategies will be discussed with the Local Authority and our partners at Wirral IT Services.
- Remote access will be password protected.

3.2 Managing filtering

The school will work with Wirral IT services to ensure systems work effectively: If staff or pupils come across unsuitable on-line materials, the site must be reported to the E-Safety Coordinator (the head teacher).

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. This will include searching for content related to inappropriate images, radicalisation and non-education content. Our Guidance on internet filtering has been updated following the introduction of the Prevent Duty in 2015.
- When headteacher checks internet filters he will e-mail DHT and Wirral IT Services to warn them the system is being tested.

3.3 E-mail

- Staff should only use school approved e-mail accounts at work. Clear guidance for what constitutes professional use of e-mail is included in the Acceptable Use agreements. However, we are absolutely clear that staff cannot use e-mail to communicate personal opinions that may be defamatory or abusive to individuals or organizations associated with the school.
- Pupils must immediately tell a teacher if they receive offensive e-mail/message.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school does not allow direct contact through personal e-mail for any professional correspondence. Any communication with other organizations, schools etc must be controlled through the teacher's e-mail account.

- The forwarding of chain letters is not permitted.

3.4 Published content and the school web site

- Staff or pupil personal contact information will not generally be published. The contact details given online should be the school office or a senior member of staff. Contact points are available on E-schools.
- The head-teacher will take overall editorial responsibility and ensure that content is accurate and appropriate. Governing Body understands their statutory duties in respect of information that should be available on the school website.

3.5 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified or their image misused. Consider using group photographs rather than full-face photos of individual children. The school will always risk assess photographs for possible abuse.
- Names or any other personal details will never be published alongside photographs.
- Pupils full names will not be used on a school Web site or other on-line space, in association with photographs.
- Work can only be published with the permission of the pupil.
- Pupil image file names will not refer to the pupil by name.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. We have an explicit permission slip for this.

3.6 Social networking and personal publishing

- The school will control access to social networking sites and consider how to educate pupils in their safe use.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Staff are fully informed of their responsibilities regarding the use of social networking sites such as Facebook. At Holy Cross Catholic Primary we have agreed that we should separate professional and personal commitments on these sites.
- All staff are aware that they could face charges of gross misconduct if they use social networking platforms to communicate personal opinions that may be defamatory or abusive to individuals or organizations associated with the school.

3.7 Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Video conferencing for pupils can only take place under the direct supervision of a member of staff.

3.8 Managing mobile technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Currently mobile phones are not to be used in school by pupils. Staff and children have explicit guidance on mobile phones (see mobile phone policy).
- The senior leadership team should note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications. **This is addressed in our mobile phones at School policy.**
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use by pupils of cameras in mobile phones is not allowed in school or on trips etc.
- Staff are not allowed to use mobile phones to take or store images.

- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.
- Staff must not take photographs on their personal phones.

3.9 Protecting and storing sensitive data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. This information will be clearly communicated to all staff, including office staff on an annual basis.

Staff are aware that they have a professional responsibility to ensure the following;

- All laptops must be password protected. Work laptops cannot be used for the storage of any inappropriate material.
- All data and images of children must be carried on encrypted memory pens. These are issued to staff.
- Photographs cannot be stored on personal laptops.
- All photographs must be stored on the school's secure Staff Drive.
- No data or images can be transported out of the school without the device being approved or password protected. This includes digital cameras etc.
- Any personal devices must be password protected if staff bring them onto school premises (Ipads, mobile phones etc).

Developing Policy on E-safety

The pace of change with emerging technology means that all staff have to be vigilant about risks concerned with e-safety. School Policy has to be proactive and clear.

The responsibility for ensuring the effective implementation of e-safety policies is the head teacher's. Individual members of staff have responsibilities under their pay and conditions to ensure that these policies are followed. Clear advice is issued by professional organisations such as the NUT, NAHT, UNISON etc on these matters.

The Governing Body will consider these matters. Many duties will be devolved to the Health and Safety Committee. The Governing Body will exercise their duty to ask the head teacher to consider any matters arising from policy reviews.

4.1 Authorising Internet access

- All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- All Parents/Carers will be asked to sign and return a consent form.
- Includes governors, visitors, student teachers etc.

4.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. The school can accept liability for any material accessed, or any consequences of Internet access.
- The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

4.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the head-teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Discussions will be held with the Police Youth Crime Officer to establish procedures for handling potentially illegal issues.

4.4 Community use of the network and Internet

- Through extended schools use and partnership with other organizations their will be wider community use of the school's network. The school will liaise with local organisations to establish a common approach to e-safety.
- All consent forms must be used for these groups.

Communicating the E-Safety Policy

5.1 Introducing the e-safety policy to pupils

- **E**-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety will be developed, possibly based on the materials from CEOP and Edu Care accredited training on online exploitation and cyber bullying.
- E-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

5.2 Staff and the E-Safety policy

- All staff will be given access to the School's E-Safety Policy and its importance explained.
- E-safety will be a focal point for staff and volunteer induction. Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils. We use google with safe filtering enabled.

5.3 Enlisting parents' and carers' support

- Parents" and carers" attention will be drawn to the School e-Safety Policy in newsletters and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

Appendix 1 : Supporting Children with Additional Needs to be E-Safe

There are many variations to school policies, populations and resources available to support e-safety initiatives within schools.

Here are some considerations regarding possible ways to support a generic group of children who may require additional support to move forward in safeguarding themselves.

- A fundamental part of teaching e-safety is to check pupil's understanding and knowledge of general personal safety issues. Some pupils may need additional teaching that includes reminders and explicit prompts to link their existing knowledge of "how to keep safe" to the rules that will apply specifically to, for instance, internet use.

- Rules are very helpful to all pupils and it is important to achieve consistency of how rules can be applied.

  - This is a difficult area for some pupils who will usually learn rules within certain contexts, but who will find it difficult to transfer these rules across environments, lessons or teachers. Schools need to consider whether a scheme or resources are applicable or accessible to all school situations where internet access may be possible.

- As consistency is so important for these pupils, there is a need to establish e-safety rules for school that are similar to those for home. Working with parents and sharing information with them would be relevant to all children, but this group especially.

- There will always be exceptions to rules and if this is the case, then these pupils will need to have additional explanations about why rules might change in different situations i.e. why it is ok to give your name and address to an adult if you are lost in town, but not when using the internet.

- It might be helpful to consider presenting the rules as being linked to consequences such that you are teaching cause-effect rather than a list of procedures. This needs to be achieved carefully so as to use realistic and practical examples of what might happen if… without frightening pupils.

How rules are presented could be vital to help these pupils understand and apply some of the rules they need to learn.

Visual support is usually important to help most pupils' understanding but some areas of this topic are quite abstract in nature and difficult to represent visually i.e.

- Uncomfortable
- Smart
- Stranger
- Friend

It might be helpful to ask pupils to produce a drawing or write a mini-class dictionary that describes and defines these words in their own terms.

- Visual support can be useful but it is more likely that the pupils will respond to multimedia presentations of the rules such as interactive power-point slides, screensavers, spoken recordings of the main rules or sounds that they can associate with decisions they make while using the internet. The really useful thing about these is the repetition and practice that pupils can have with these which may not be so easy if spoken language were used.

- If visual prompts are used to help remember the rules, the picture or image support needs to give the pupils some improved understanding of what the rule is about. It is quite easy to find attractive pictures that link to other abstract ideas not related to internet use i.e. use of a compass to show "lose track" of a search when a head looking confused is more like what happens.

- This group of pupils are vulnerable to poor social understanding that may leave them open to risks when using the internet individually, but also when with peers.

  - It can be common for peers to set up scenarios or "accidents" regarding what they look for on the internet and then say it was someone else who has done so. Adults need to plan group interactions carefully when raising awareness of internet safety.

  - Some pupils in this group may choose recreational internet activities that are perhaps simpler or aimed at pupils younger than themselves. By their very nature, these activities tend to be more controlled and less open to naïve mistakes. Staff need to plan how to manage pupils who may want to do the same as other peers but who may need small step teaching due to limited experiences with internet use

- For various reasons, pupils with additional needs may find it difficult to explain or describe events when using the internet

  - Some pupils might find it easier to show adults what they did i.e. replay which will obviously have it's own issues for staff regarding repeating access

- Some pupils are very quick to click with the mouse and may not actually know what they did or how something happened. Gentle investigation will be more productive than asking many questions.

- Some may not be able to ask for help. Staff will need to know specific pupils well so that this can be addressed.

  - Pupils may need a system or a help sound set up on computers which will help them to get adult attention. If pupils don't recognise that they need help, then adult supervision is the safe way to improve their recognition of this.

Useful websites for resources

www.gridclub.com

www.kidsmart.org.uk

www.thinkuknow.co.uk www.netsmartz.org

www.bizzikid.co.uk **Appendix 2:**

Internet use - Possible teaching and learning

activities Appendix 2: NSPCC

Share Aware

We use the resources from the NSPCC to signpost and support families. Some of their key resources are below:

Family Online Agreement:

Our family online agreement

Creating a family agreement is a great way to start conversations about online safety and to discuss any worries you may have. Make sure you review the rules together regularly to keep them up-to-date.

..... agree(s) to:

(eg check before I download a new app)

..... agree(s) to:

(eg ask my child's permission before posting photos of them on social media)

We both agree to:

(eg talk about what we're up to in our online world like our offline world)

SIGNED .....

SIGNED .....

For more information search **'Share Aware'**

O2 NSPCC

Let's keep kids safe online

Tips to help keep your child safe online

Helpful tools and advice you can use to keep your child safe when they use the internet at home, at a friend's house or at school.

The internet is great for learning, sharing, connecting and creating. So try and balance how you guide your child on online safety with an understanding of why they want to use it. You don't want your child to feel they can't come to you if they encounter a problem online.

Set rules and agree boundaries as a family

- ✓ Set boundaries for how long your child can spend online and what they can do.
- ✓ Agree this as a family so that access to devices can be shared fairly.
- ✓ Remember there are tools that can help you manage and monitor access and use across all devices.

Talk about online safety and get involved

- ✓ Have conversations about online safety little and often and build it into other conversations.
- ✓ Ask questions about what they do online, such as what sites they visit and who they talk to.
- ✓ Make the use of the internet a family activity.
- ✓ Remember to share these rules with babysitters, childminders and other family members.
- ✓ Talk to other parents about internet use, such as what they do and don't allow.

Appendix 3: **Holy Cross Catholic Primary School Agreed Staff Code of Conduct to promote E-Safety and Responsible Use**

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. This school expects that all activity should be related to a professional use.

I appreciate that ICT includes a wide range of systems, including mobile phones, tablet computers, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business. It is my responsibility to ensure that I do not store any inappropriate material on these devices in school.

I understand that school information systems may not be used for private purposes without specific permission from the head teacher.

I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance. This is managed by Wirral IT Services internet filtering.

I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.

I will not install any software or hardware without permission.

I will ensure that personal data is stored securely 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 e-Safety Coordinator and the Designated Child Protection Coordinator.

I will ensure that electronic communications with pupils and parents including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete 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.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed:_____ Date: _____

THINK before you CLICK

We only use the Internet when an adult is with us

Click on buttons and links ONLY when you know what they do

We can search the Internet with the help of an adult

We always ask if we get lost on the Internet

We can send and open emails together

Appendix 5 – **Key Stage 2 E-Safety Rules**

Think then Click

We ask permission before using the Internet.

We only use websites our teacher has chosen.

We immediately close any webpage we don't like

We only e-mail people our teacher has approved

We send e-mails that are polite and friendly.

We never give out a home address or phone numb

We never arrange to meet anyone we don't know

We never open e-mails sent by anyone we don't kn

We never use Internet chat rooms.

We tell the teacher if we see anything we are unhapp

J. Barrett & H. Barton

Appendix 6 – **Permission Letter for Network and Internet Use**

Holy Cross Catholic Primary School

E- Safety Consent Form

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

Our E-safety policy is available from the school office and is published on the school's website.

Pupil:	**Year Group:**

Pupil's Agreement

- I have read and I understand the school e-Safety 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.

Signed:	**Date:**

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. 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.

Parent's Consent for Internet Access

I have read and understood the school e-safety 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 pupils 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.

Signed:	**Date:**
Please print name:	

Please complete, sign and return to the School Office

Appendix 7: **Consent Form for Visiting Adults Using our Network and Internet Access**

All adults have to responsible when using information systems. As visitors to schools, adults have to be aware that their activities must be related to education or their role within the school. Any abuse of this privilege could result in access being removed. In cases where the school feels that either their pupils or staff have been placed at risk, this could lead to the incident being reported to the police.

All visitors should consult the school's e-safety policy for further information and clarification. This is available through the school office or the school's website.

I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. This school expects that all activity should be related to a professional and educational use.

I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business. It is my responsibility to ensure that I do not store any inappropriate material on these devices in school.

I understand that school information systems may not be used for private purposes without specific permission from the head teacher.

I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.

I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.

I will not install any software or hardware without permission.

I will ensure that no files are removed from the school's network without the express permission of a senior member of the school's staff.

I will respect copyright and intellectual property rights.

I will report any incidents of concern regarding children's safety to the Headteacher.

I will ensure that all e-mail communication is appropriate.

I will not access any inappropriate websites including social networking sites.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete 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.

I have read, understood and accept the Visitor's Code of Conduct for ICT.

Signed:_____ Date: _____

Appendix 8

E-Safety Audit – Holy Cross Catholic Primary School

This self-audit should be completed by the member of the Senior Leadership Team (SLT) responsible for e-safety policy. Many staff could contribute to the audit including: Designated Child Protection Coordinator, SENCO, e-Safety Coordinator, Wirral IT Service and Headteacher.

Has the school an e-Safety Policy that complies with Wirral LA guidance?	**Y/N**
Date of latest update (at least annual):	
The school e-safety policy was agreed by governors on:	
The policy is available for staff at:	
The policy is available for parents/carers at:	
The responsible member of the Senior Leadership Team is:	
The responsible member of the Governing Body is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Has e-safety training been provided for both pupils and staff?	**Y/N**
Is there a clear procedure for a response to an incident of concern?	**Y/N**
Have e-safety materials from CEOP and Becta been obtained?	**Y/N**
Do all staff sign a Code of Conduct for ICT on appointment?	**Y/N**

Are all pupils aware of the School's-Safety Rules?	**Y/N**
Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all pupils?	**Y/N**
Do parents/carers sign and return an agreement that their child will comply with the School e-Safety Rules?	**Y/N**
Are staff, pupils, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	**Y/N**
Has an ICT security audit been initiated by SLT, possibly using external expertise?	**Y/N**
Is personal data collected, stored and used according to the principles of the Data Protection Act?	**Y/N**
Is Internet access provided by an approved educational Internet service provider which complies with DCSF requirements ?	**Y/N**
Has the school-level filtering been designed to reflect educational objectives and approved by the School's Leadership Team?	**Y/N**