Holy Family Catholic Primary School

E-Safety Policy

We live, love and learn together in the light of God by…
praying together
learning together
playing together
and
respecting each other

RATIONALE

Providing access to the internet in school contributes towards the raising of standards and supports the professional work of staff. The dangers and risks associated with the increasing use of ICT in school demand an informed and skilled staff supported by governors and parents to ensure pupil safety at all times.

CONTEXT

This policy addresses a number of technical, educational and significant changes and developments in recent years have occurred in all areas of the curriculum.

Whilst recognising that the use of ICT in school is of great benefit to pupils, the school must still address e-Safety issues and plan accordingly to ensure appropriate, effective and safe use of electronic communications management issues.

INTERNET ACCESS IN SCHOOL

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.

The internet is also be used to enhance the school's management information and business administration systems.

Staff, including supply staff, will not be expected to take charge of an internet activity without training. Staff should be given opportunities to discuss the issues and develop good teaching strategies. All staff, (including teachers, supply staff, classroom assistants, students and lunchtime supervisors), and any other adults involved in supervising children accessing the internet, will be provided with this policy, and will have its importance explained to them.

In our school we have staff, Governors and parents who are also parents of children in the school and therefore have friends who are parents. If staff, Governors or volunteers are signed up to social networking sites such as Facebook that is completely their right; however, as members of staff working in a professional context they need to be careful with what they share and with whom. Social networking site comments between friends could lead to a potential conflict of interest which could mean staff are in breach of their contract.

School staff will not invite, accept or engage in communications with parents or children from the school community to any personal social networking sites while in employment at Holy Family School.

Parents' attention will be drawn to the Policy and will be available for parents and others to read on request.

MANAGING THE SCHOOL INFORMATION SYSTEM

The security of the school information systems and users will be reviewed regularly and Virus protection regularly updated.

- Personal data sent over the Internet or taken off site will be encrypted.
- Portable media may not used without specific permission from the E-Safety Officer followed by a virus check.
- Files held on the school's network will be regularly checked.
- The ICT coordinator/network manager will review system capacity regularly.
- No personally owned equipment may be used in school, (including cameras and video equipment), without the permission of the E-Safety Officer.

USING INFORMATION FROM THE INTERNET

In order to use information from the internet effectively, it is important for pupils to develop an understanding of the nature of the internet and the information available on ICT. In particular, they should know that most of the information on the internet is intended for an adult audience.

Staff will ensure that pupils are aware of the need to validate information whenever possible before accepting ICT as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium).

When copying materials from the Web, pupils will be taught to observe copyright.

Pupils will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed.

Pupils will be taught to treat search engines such a Google with respect and to understand that the information contained in sites that they visit may not be accurate.

MANAGEMENT OF E-MAIL

- Pupils will only be allowed to use e-mail once they have been taught the Rules of Responsible Internet Use, (appendix i), and the reasons for these rules.
- Staff will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using e-mail;
- Pupils will only be able to send internal emails or to addresses that have been permitted by the safety officer.
- In-coming e-mail to pupils will not be regarded as private;
- Pupils will have the e-mail messages they compose checked by a member of staff before sending them;

- The forwarding of chain letters will not be permitted;

PUBLISHING ON THE INTERNET
THE SCHOOL WEBSITE

Our school web site is intended to:

- Provide accurate, up-to-date information about our school;
- Enable pupils to publish work to a high standard, for a very wide audience including pupils, parents, staff, governors, members of the local community and others;
- Celebrate good work;
- Provide pupils with the opportunity to publish their work on the internet;
- Promote the school.

All classes may provide work for publication on the school web site. Staff will be responsible for ensuring that the content of the pupils' work is accurate and the quality of presentation is maintained. All material must be the author's own work, crediting other work included and stating clearly that author's identity and/or status. The SLT in conjunction with the site administrator (Arrowscape) is responsible for ensuring that the links work and are up-to-date, and that the site meets the requirements of the site host.

The point of contact on the web site will be the school address, telephone number and e-mail address. We do not publish pupils' full names or photographs that identify individuals on our web pages. Home information or individual e-mail identities will not be published. Staff will be identified by their title and surname unless they request otherwise. Permission will be sought from other individuals before they are referred to by name on any pages we publish on our web site.

- Email addresses should be published carefully, to avoid being harvested for spam (e.g. replace '@' with 'AT'.
- The E-Safety Officer will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

PUBLISHED WORK AND IMAGES

- Images 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.
- Parents have the right to ask that images of their children or their children's

work are not published on the internet.

MANAGEMENT OF SOCIAL MEDIA AND PERSONAL PUBLISHING

- The school will strictly control access to social media and social networking sites.
- The school recognises that some pupils may have access at home to social media sites. Pupils will, therefore 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 and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils should 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. Advice should be given regarding background detail in a photograph which could identify the student or his/her location.
- If personal publishing is to be used with pupils then it must use age appropriate sites suitable for educational purposes. Personal information must not be published and the site should be moderated by school staff.

FILTERING

- The school system is protected by a Firewall which is regularly updated. The school also has Policy Central monitoring software in place to detect any malicious use of internet provision.
- This is checked regularly by members of the SLT – any student misusing the internet will be disciplined by the SLT depending in the extent of misuse.
- Any misuse of the internet by staff will be passed on the Deputy Headteacher.

VIDEO CONFERENCING

Videoconferencing enables users to see and hear each other between different locations. This 'real time' interactive technology has many uses in education.

Equipment ranges from small PC systems (web cameras) to large room based systems that can be used for whole classes or lectures.

- Videoconferencing contact information should not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment should not be taken off school premises without permission.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be closely supervised at all times and will only take place with known individuals/organisations, (eg other

schools).

MANAGEMENT OF EMERGING TECHNOLOGIES

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration and multimedia tools. A risk assessment will be undertaken on each new technology for effective and safe practice in classroom use to be developed.

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

PROTECTING PERSONAL DATA

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused.

The Data Protection Act 1998 ("the Act") gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information (personal data) must notify the Information Commissioner's Office, unless they are exempt.

The Data Protection Act 1998 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals. The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

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.

INTERNET ACCESS RULES & SEARCH ENGINE USE

- 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 Acceptable use policy statement before accessing the school's ICT system, (appendix ii).
- The Rules of Responsible Internet Use, (appendix i), should be explained to all pupils before they are allowed internet access
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved online materials.
- Parents/Carers will be informed that pupils will be provided with supervised Internet access

Where Key Stage 2 pupils are allowed access to internet search engines they should be made aware of the possibility of inadvertently accessing inappropriate or inaccurate information and that this must be report immediately to the teacher in charge.

Although the filtering system/firewall does stop most undesirable material, it is not always as effective when searching for images. Pupils should be directed to the following, more suitable websites for this purpose:

www.askkids.com, **www.picsearch.com** or **www.bing.com**

ASSESSMENT OF RISK

- 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. The school cannot accept liability for the material accessed, or any consequences resulting from inappropriate internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

COMPLAINTS AND MISUSE

Parents, teachers and pupils should know how to use the School's complaints procedure. The facts of the case will need to be established, for instance whether the Internet use was within or outside school.

A minor transgression of the rules may be dealt with by a member of staff. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's disciplinary policy. Potential child protection or illegal issues must be referred to the school Designated Child Protection Coordinator or E-Safety Officer.

- Complaints of Internet misuse will be dealt with under the School's Complaints Procedure.
- **Staff should be aware that misuse of the ICT system could constitute a disciplinary offence**
- Any complaint about staff misuse must be referred to the headteacher.
- All e-Safety 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.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

PREVENTION OF CYBERBULLYING

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

Many young people and adults find using the internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also being used negatively. When children are the target of bullying via mobiles phones, gaming or the internet, they can often feel very alone, particularly if the adults around them do not understand cyberbullying and its effects. A once previously safe and enjoyable environment or activity can become threatening, harmful and a source of anxiety.

It is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

DCSF and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

Cyberbullying (along with all forms of bullying) will not be tolerated in school.

- All incidents of cyberbullying reported to the school will be addressed (see HFCS Antibullying Policy).
- There will be clear procedures in place to investigate incidents or allegations of Cyberbullying:
- Pupils, staff and parents/carers will be 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 may be informed.
- The Police will be contacted if a criminal offence is suspected.

INTERNET EDUCATION

The teaching of safety is an integral part of the computing curriculum that is delivered in Holy Family. Staff are provided with safety teaching opportunities for each unit of work delivered as part of the Rising Stars Switched On scheme.

Useful e-Safety programmes include:

- Think U Know: ***www.thinkuknow.co.uk***
- Childnet: ***www.childnet.com***
- Kidsmart: ***www.kidsmart.org.uk***
- Safe Social Networking: ***www.safesocialnetworking.com***

Parents will be regularly updated about the risks associated with the internet through regular e safety briefings. Where possible local police will support with this.

INTERNET ACCESS AND HOME/SCHOOL LINKS

Parents will be informed that pupils are provided with supervised internet access as part of their lessons. We will keep parents in touch with future ICT developments by letter and newsletter.

School and Local Authority guidelines on issues such as safe internet use will be made available to parents together with printed information and internet sites providing information for parents about safe access for children.

This Policy should be read in conjunction with HFCS Internet Access Policy.

Signed: _____ Chair of Governors

Date _____ September 2015

Rules of Responsible Internet Use

The school has provided computers to help you to learn more effectively. Although computers can be fun, they can sometimes be harmful if they are not used properly. It is important that you follow these rules:

Equipment

- Never eat or drink near to the computer equipment
- Computers may only be used with the permission of a member of staff

Security and Privacy

- Never use someone else's logon name or password
- Remember that staff are able to look at what you are doing, or have done, on the computer

Internet

- You may only access the internet with the permission of a member of staff
- Report any inappropriate images or text to an adult immediately
- Respect laws of copyright – your teacher will tell you about these
- Do not access chat rooms or other social media in school
- Remember that people who you 'meet' on the internet are not always who you think that they are

Email

- You may only use e-mail addresses that you are given permission to use by your teacher
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff.

If you do not follow these rules then you may not be allowed to use the internet in school and other action may also be taken.
(Appendix i)

Holy Family School Acceptable Use Policy

The computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. To ensure the safety of all children and staff it is important that the following policy is adhered to:

Equipment

- Always get permission before installing, attempting to install or storing programs of any type on the computers.
- Always check files brought in on removable media (such as floppy disks, CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.
- Always check mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Always be wary about revealing your home address, telephone number, school name, or picture to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- A member of the SLT may review your files and communications to ensure that you are using the system responsibly.

Internet

All members of staff should read HFCS E-Safety Policy which clearly explains appropriate and acceptable use of the internet by staff employed at the school.

- Within directed time you should access the Internet only for preparation and planning for teaching and learning activities.
- Use of the internet for any other reasons is not allowed.

- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- 'Chat' activities take up valuable resources which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons 'chat' rooms must not be visited.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet will be denied and you will be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Name: _____ Signature: _____

All computer users are required to accept the following statement when they log on to a school computer inside or outside school.

This computer network has an Acceptable Use Policy (AUP) related to all computer, related equipment, network and internet use.

Any such use which is found to include inappropriate, suggestive, confidential or illegal material to the detriment of it's owners or other users and which has been transmitted, received or created on this computer is a violation of the AUP.

Any individual found to be in violation of this AUP will be subject to disciplinary action.

The computer, related equipment, network and internet is not for personal use during the hours of 8:00 - 12:00 and 13:00 - 15:15.

If you do not understand the information contained in this policy, please contact a member of management immediately.