Holy Family Catholic Primary School

E-Safety Policy 2019

Background Summary

Liverpool City Council firmly believes that the effective use of information and communication technologies in schools can bring great benefits. Recognising the e-Safety issues and planning accordingly will help to ensure appropriate, effective and safer use of digital technologies. It is hoped that this policy template will help schools and settings to review their approach to e-Safety and where necessary update their policy and practice. This exemplar policy has been written to take account of e-safety across a range of educational settings so it is expected that an individual setting will ensure that it is adapted to meet their needs.

Liverpool City Council must gratefully acknowledge the support and guidance that it received from the Safer Internet Centre, The South West Grid for Learning, The UK Council for Child Internet Safety and Childnet when writing this policy.

Holy Family Catholic Primary School has adopted this policy to meet our needs.

1. Development/Monitoring/Review of this Policy

This e-Safety policy has been developed by a working group made up of:

- School E-Safety Coordinator
- Headteacher / Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- Governors
- Parents and Carers

Designated Safeguarding Lead (DSGL)– Head	Rachel Davidson (Headteacher)
Deputy DSGL	Angela Snell/Jacquie Clein
Computing Subject Leader	Liz Doherty
Responsibility for e-safety	Liz Doherty
E-Safety Governor	
Safeguarding Governor	

Monitoring will take place at regular intervals:	
The Governing Body / Governors Sub Committee will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or	Nov '19

The implementation of this e-safety policy will be monitored by the Senior Leadership Team

incidents that have taken place. The next anticipated review date will be:	
This E-safety policy was approved by the Governing Body/Governors Sub Committee on:	

2. Scope of the Policy

This policy applies to all members of our school community (staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of the school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place inside and outside of Holy Family Catholic Primary.

3. Context

We live in a digital age where technology is playing an ever increasing part in our lives; it is changing the way that we do things both inside and outside of school and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, pupils and parents/carers associated with the school are able to use technology in a safe and responsible manner.

Some of the potential dangers of using technology may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the offline world but it is important that as a school we have a planned and coordinated approach to ensuring that all involved with the school use technology in a safe and responsible way. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

The school have adopted the PIES model which is the basis of it approach towards E-Safety and helps to manage and minimise its risk.

1) Policies and practices

The e-Safety policy outlines the importance of ICT within and outside of education. It provides guidance on the schools approach to E-Safety and details a code of conduct for school staff and pupils. The policy aims to provide an agreed, coordinated and consistent approach to E-safety. The code of conduct forms the basis of Holy Family's expected behaviours regarding the use of technology and any infringements of the code of conduct will lead to disciplinary action against the perpetrator(s).

2) Infrastructure and technology

The schools educational network and access to the internet is provided by BT. This network provides a safe and secure broadband connection to the internet. There is a Universal Threat Management security shield that provides dual-layer firewall protection, intruder detection/prevention, load balancing, content caching, data traffic analysis and virus protection. This is provided by Smoothwall . Smoothwall undertakes live scanning of all sites and blocks any threats or inappropriate websites. The infrastructure has been designed to minimise the risk of; users accessing inappropriate material, data being lost or accessed by unauthorised users, virus or malware threats. All internet and network activity is logged via the Smoothwall Dashboard and can be retrieved if required in the event of an investigation.

The school is responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible.

3) Education and training

As the use of technology and the potential risks associated with the use of the technology change rapidly, it is essential to ensure that the school community know how to use technology safely and responsibly. At Holy Family, we are committed to ensuring that staff receive regular training to keep up to date with new developments and ensure that they are sufficiently confident to educate pupils in the safe and responsible use of technology. The school have designed an E-safety curriculum that meets the needs of all pupils and ensure their safety and well-being. The curriculum is reviewed and revised on a regular basis to ensure that it remains current. The school will also endeavour to provide information and training opportunities for parents and carers to raise their awareness of the technologies that their children are potential using and the risks that they potentially face.

4) Standards and inspection

The school reviews its approach to E-safety on a regular basis and uses the 360° Safe tool to evaluate and improve its provision. Reference is also made to e-safety in the annual 175 audit and through Ofsted inspections.

4. Policy Statements

Whilst the PIES model forms the basis of the schools approach to E-safety the school will ensure that all access to the internet and ICT systems by pupils is effectively managed and supervised.

As part of the E-safety policy the school will also manage:

- The use of digital images and video
- Data protection
- Digital communications
- Unsuitable/inappropriate activities
- Incidents of misuse

The use of digital images and video

The development of digital imaging technologies has created significant benefits to learning, allowing school staff and pupils instant use of images they have recorded themselves or downloaded from the internet. At Holy Family, staff and pupils are made aware of the potential risks associated with storing, sharing and posting images on the internet and must follow the good practice detailed below.

- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are permitted to take digital images and video to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes.
- Care will be taken when capturing digital images and video that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Images and videos published on the school website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work will only be published with the permission of the pupil and parents or carers.

Data Security and Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

All school staff will ensure that:

- Care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Personal data is used or processed on only secure password protected computers and other devices and that these devices are properly "logged-off" at the end of any session in which they are using personal data.
- Data is transferred securely using encryption and secure password protected devices and email solutions.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - the data must be encrypted and password protected
    - the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
    - the device must offer approved virus and malware checking software
    - the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Digital Communication

Digital communication is an area that is developing rapidly with new and emerging technologies, devices are becoming more mobile and information sharing/communication is becoming more sophisticated.

When using communication technologies the school ensures the following good practice:

- The official school email service is regarded as safe and secure and is monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, on school business or on school systems. (@holyfamily.liverpool.sch.uk)
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, pupils or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored)

school systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.

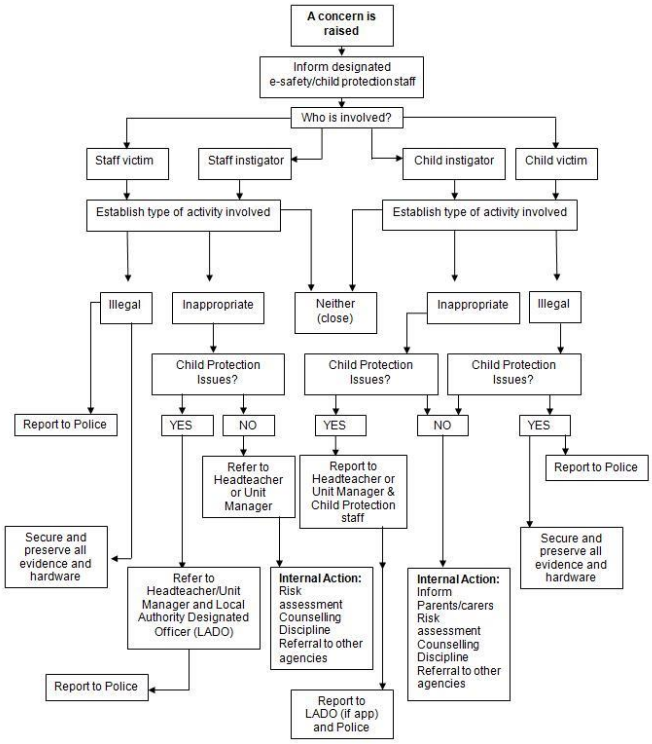
- Whole class or group email addresses will be used at Key Stage 1, while pupils at Key Stage 2 and above will be provided with individual school email addresses for educational use.
- Pupils will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.

Unsuitable/inappropriate activities

School ICT systems are only to be used for agreed, appropriate and suitable work related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegal will be reported and could lead to criminal prosecution.

Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place accidently, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of an e-safety incident it is important that there is a considered, coordinated and consistent approach. Incidents will be managed using the incident flowchart below.



All incidents will be recorded and reported to the relevant parties and organisations.

Holy Family Staff/Volunteer Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images

are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff/Volunteer Name _____

Signed _____

Date _____