Holy Family Catholic Primary School

E-Safety & Computer Acceptable Use Policy

Mission Statement

We live, love and learn together in the light of God by…

praying together

learning together

playing together

and

respecting each other

Approved by:	Linda Mockler	**Date:** 11th July 2024	
Next review due by:	July 2025		

RATIONALE

Holy family provides access to the internet in school which contributes towards the raising of standards and supports the professional work of staff. We embrace the positive impact and educational benefits that can be achieved through appropriate use of the Internet and associated Communications technologies. The dangers and risks associated with the increasing use of Computing 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 Computing 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. A separate E-Safety curriculum has been implemented across the school so children are educated on the appropriate use of internet and associated communications technologies.

DEVELOPMENT/REVIEW OF THIS POLICY

This E-safety policy has been developed by the Digital Council made up of:

• SLT

• E -Safety Coordinator

• Staff – including Teachers, Support Staff, Technical staff

• Governors

• Parents and Carers

• Community users

Consultation with the whole school community has taken place through a range of

formal and informal meetings.

INTERNET ACCESS IN SCHOOL

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

PUBLICISING E-SAFETY

Effective communication across the school community is key to achieving the school vision for safe and responsible citizens. To achieve this we will:

· Make this policy, and related documents, available on the school website at:

http://www.holyfam.bham.sch.uk

· Introduce this policy, and related documents, to all stakeholders at appropriate times. This will be at least once a year or whenever it is updated

· Post relevant E- Safety information in all areas where computers are used

· Provide E- Safety information at parents' evenings and to pupils through assemblies and workshops.

ROLES AND RESPONSIBILITIES

The following section outlines the E-Safety roles and responsibilities of individuals and groups within the school.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about E-Safety incidents and monitoring reports. A member of the Governing Body / Board has taken on the role of E- Safety Governor:

• Regular meetings with the E-Safety Co-ordinator

• Regular monitoring of E-Safety incident logs from CPOMS

• Regular monitoring of filtering / change control logs

Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Co-ordinator.

· The Headteacher and (at least) another member of the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious E-Safety allegation being made against a member of staff.

· The Headteacher / Senior Leaders are responsible for ensuring that the E Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.

· The Headteacher / Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal E-Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

· The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Co-ordinator

· leads the E-Safety committee (Digital Council)

· takes day to day responsibility for E-Safety issues and has a leading role in establishing and reviewing the school E-Safety policies / documents

· ensures that all staff are aware of the procedures that need to be followed in the event of an E-Safety incident taking place.

· provides training and advice for staff

· liaises with the Local Authority / relevant body

· liaises with school technical staff

· receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments

· meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs

· Reports regularly to Senior Leadership Team

Office Manager/ IT Technicians

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

Cyber Attacks are responded to following the guidance of Cyber Response Plan (See policy approved March 2023)

•Personal data sent over the Internet or taken off site will be encrypted.

•Portable media may not be 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 Computing co-ordinator/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.

Digital Council

The Digital Council (E-Safety Group) provides a consultative group that has wide representation from the school community, with responsibility for issues regarding E-Safety and the monitoring the E-Safety policy including the impact of initiatives. Depending on the size or structure of the school this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the Digital Council will assist the E-Safety Co-ordinator with:

· the production / review / monitoring of the school E-Safety policy /

documents.

· mapping and reviewing the E-Safety curricular provision – ensuring relevance, breadth and progression

· monitoring network / internet / incident logs

· consulting stakeholders – including parents / carers and the students about the E-Safety

provision

· monitoring improvement actions identified through use of the 360 degree safe self-review tool

Teaching and Support Staff

· They have an up to date awareness of E-Safety matters and of the current school E-Safety policy and practices

· They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)

· They report any suspected misuse or problem to the Headteacher / Senior Leader ; E-Safety Co-ordinator for investigation / action / sanction

· All digital communications with students / parents / carers should be on a professional level and only carried out using official school systems

· E-Safety issues are embedded in all aspects of the curriculum and other activities

· Students understand and follow the E- Safety and acceptable use policies

· Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

· They monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

· In lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Child Protection / Safeguarding Designated Officer

. Should be trained in E-Safety issues and be aware of the potential for

Serious child protection / safeguarding issues to arise from:

· Sharing of personal data

· Access to illegal / inappropriate materials

Pupils

· are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy

· have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

· need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

· will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

· should understand the importance of adopting good E- Safety practice when using digital technologies out of school and realise that the school's E- Safety Policy covers their actions out of school, if related to their membership of the school

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 Computing. 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 Computing 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 through the E-Safety curriculum.

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 through the E-Safety curriculum.

KS2 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 through the E-Safety curriculum.

EDUCATION

Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. At Holy Family, the education of students in E-Safety is therefore an essential part of the school's E-Safety provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and build their resilience. Holy Family commits to E-Safety in all areas of the curriculum and staff reinforce E-Safety messages across the curriculum. The E-Safety curriculum is broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

• A planned E-Safety curriculum is provided as part of Computing / PHSE / other lessons and will be regularly revisited
• Key E-Safety messages are be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
• Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
• Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Pupils will be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
• Staff will act as good role models in their use of digital technologies the internet and mobile devices
• In lessons where internet use is pre-planned, it is best practice that students will be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
• Where pupils are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.
• It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Parents / carers

Many parents and carers have only a limited understanding of E-Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Holy Family will therefore seek to provide information and awareness to parents and carers through:
• Letters, newsletters, website
• Parents evenings / sessions
• High profile events / campaigns eg Safer Internet Day

The Wider Community

The school will provide opportunities for local community groups / members of the community to gain from the school's E-Safety knowledge and experience. This may be offered through the following:
• Providing computer classes to improve computer knowledge and understanding.
• The school website will provide E-Safety information for the wider community

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.

DIGITAL AND VIDEO IMAGES PERMISSION

- 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.
- Incident book for E-Safety incidents.
- Any E-Safety incidents will be reported to the DSL using MyConcern.

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).

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Communication Technologies	Staff and other adults				Pupils			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission and supervision	Not allowed
Mobile phones may be brought to school	/						/	
Use of mobile phones in lessons				/				/
Use of mobile phones in social time	/							/
Taking photos on mobile phones / cameras		/						/
Use of other mobile devices eg tablets, gaming devices		/					/	
Use of personal email addresses in school, or on school network		/						/
Use of school email for personal emails				/				/
Use of messaging apps				/				/
Use of social Media		/					/	

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) – contrary to the Public Order Act 1986					X
remarks, proposals or comments that contain or relate to: pornograph					
promotion of any kind of discrimination				X	
threatening behaviour, including promotion of physical violence or mental harm				X	
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Other User actions				X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non educational)			X		

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 2018 ("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 2018 is the UK's implementation of the General Data Protection Act 1998 (GDPR) and 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.

- IT Technicians admin handover, passwords need to be changed to reduce data loss.

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 Computing 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** **www.bing.com** or **www.kidstube.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.

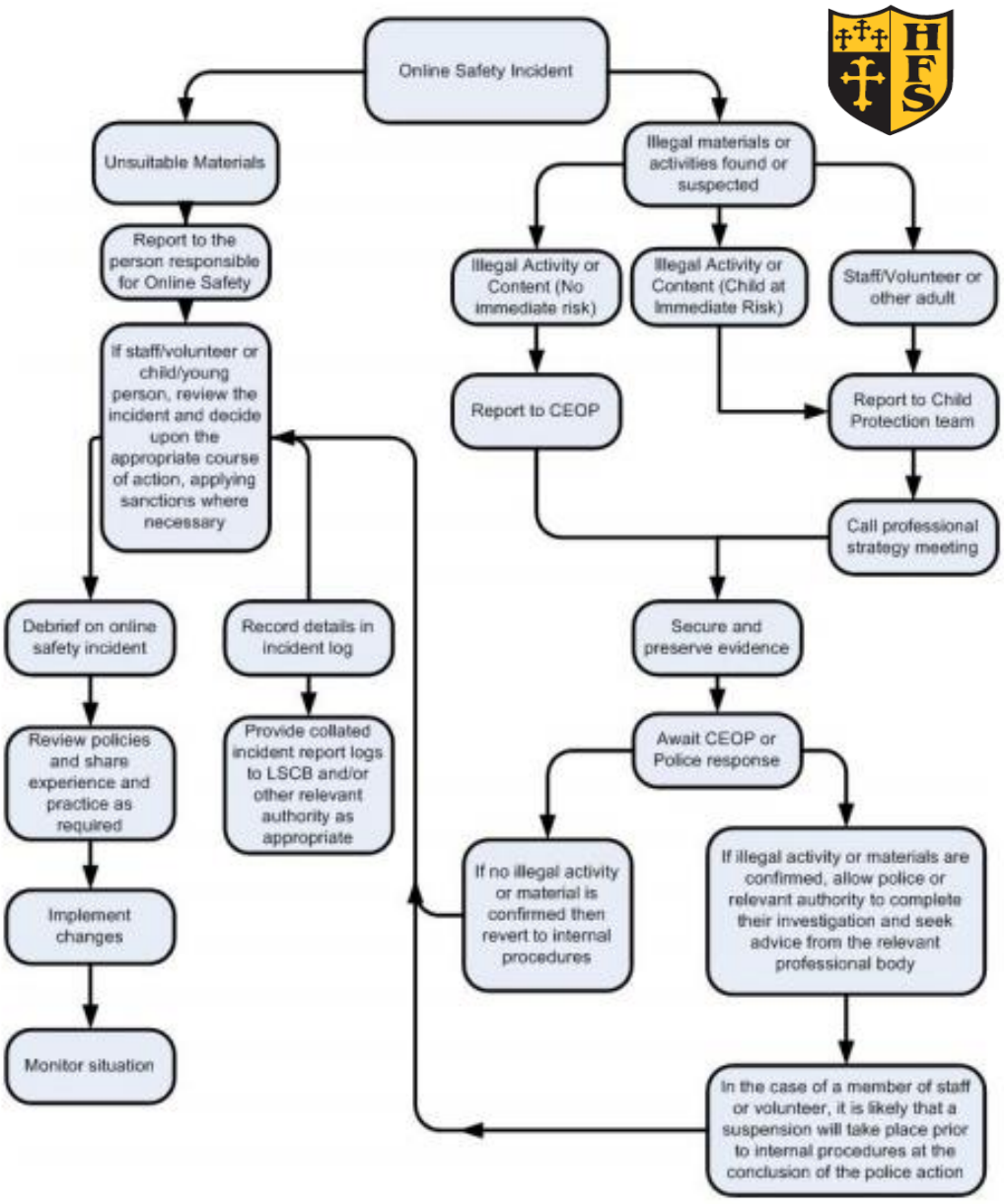
COMPLAINTS AND MISUSE

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.

- **Staff should be aware that misuse of the Computing 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.

The flowchart below describes Holy family's action towards E-Safety Incidents.



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 Positive Behaviour & Discipline 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 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 Computing 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 Computer & Internet Acceptable use Policy attached.

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)

Acceptable Use Policy for KS1

I want to feel safe all the time. I agree that I will:

Always keep my passwords a secret

Only open pages which my teacher has said are OK

Only work with people I know in real life

Tell my teacher if anything makes me feel scared or uncomfortable

Make sure all messages I send are polite

Show my teacher if I get a nasty message

Not reply to any nasty message or anything which makes me feel uncomfortable

Not give my mobile phone number to anyone who is not a friend in real life

Only email people I know or if my teacher agrees

Only use my school email / school cloud services

Talk to my teacher before using anything on the internet

Not tell people about myself online (I will not tell them my name,

Anything about my home and family and pets)

Not load photographs of myself onto the computer

Never agree to meet a stranger

Anything I do on the computer may be seen by someone else!

Acceptable Use Policy for KS2

When I am using the computer or other technologies, I want to feel
Safe all the time. I agree that I will:

Always keep my passwords a secret
Only visit sites which are appropriate to my work at the time
Work in collaboration only with friends and I will deny access to others
Tell a responsible adult straight away if anything makes me feel scared
Or uncomfortable online
Make sure all messages I send are respectful
Show a responsible adult if I get a nasty message or get sent anything
That makes me feel uncomfortable
Not reply to any nasty message or anything which makes me feel
Uncomfortable
Not give my mobile phone number to anyone who is not a friend
Only email people I know or those approved by a responsible adult
Only use email / cloud services which have been provided by school
Talk to a responsible adult before joining chat rooms or networking sites
Always keep my personal details private (my name, family information,
Journey to school, my pets and hobbies are all examples of personal
Details).
Always check with a responsible adult and my parents before I show
Photographs of myself
Never meet an online friend without taking a responsible adult that I
Know with me

I know that once I post a message or an item on the internet then it is completely out of my control.
I know that anything I write or say or any website that I visit may be being viewed by a responsible adult.

Acceptable Use Policy for Adults Working With Young People

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within

School 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.

As the digital world increasingly becomes a greater part of the learning environment instances of internet misuse are ever on the rise, along with opportunities to access harmful content such as extremist messages, pornography and other illegal content. A real risk to children and young people in the UK today is the process of radicalisation. The internet provides a powerful communications mechanism where young people can be reached, groomed and influenced. The internet is a key source of information and propaganda for extremist beliefs, meaning that young people can gain access to powerful messages, video and imagery that help to support political claims made by extremists. The internet acts as an 'echo chamber' providing an environment where otherwise unacceptable views and behaviour become normalised through on-going support and encouragement. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

That staff, volunteers and other adults working with young people 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. That staff are committed to educating and supporting young people to ensure they remain safe online.

The Community Trust will try to ensure that staff and volunteers have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff, volunteers and other adults working with young people 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 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. I will work to reduce the appeal of online propaganda and extremist messages by ensuring the young people in my care are media literate and able to assess whether material found on line is from a trusted source.

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 (e.g. laptops, email, cloud services etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.

I understand that the school ICT systems are primarily intended for educational use and I will only use the systems for this purpose.

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 understand that I should set strong passwords (a password which uses a combination of letters, numbers and other permitted symbols). I will not write down or store a password where it is possible that someone may steal it.

I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to a lead person for E-Safety using an E-Safety concern form.

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. Where these images are published (e.g. on the school website, twitter etc.) 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 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 Community Trust have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

I will follow, adhere to and positively promote any supplied E-Safety guidance.

I will not use personal email addresses on the school ICT systems.

I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).

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.

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 Trust Data Protection Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and restricted data must be held in lockable storage.

I understand that the Trust 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 to the schools ICT service desk.

When using the internet in my professional capacity:

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 system and equipment in school, but also applies to my use of school ICT systems and equipment off the premises.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action and in the event of illegal activities the involvement of the police.

I confirm that I have read and understand the above, and agree to use the school ICT systems (both in and out of school) within these guidelines.

Name: _____

Signature: _____ Date: _____

Acceptable Use Policy for Our Schools & Trustees

This policy aims to ensure that any communications technology (including computers, mobile devices/phones etc.) is used to supporting learning without creating unnecessary risk to users.

The Board of Trustees will ensure that:

Learners are encouraged to enjoy the safe use of digital technology to enrich their learning
Learners are made aware of risks and processes for safe digital use
All adults and learners have received the appropriate acceptable use policies and any required training
The school has appointed an E-Safety Lead and a named Trustee takes responsibility for E-Safety
An E-Safety Policy has been written by the school
The E-Safety Policy and its implementation will be reviewed annually
The school internet access is designed for educational use and will include appropriate filtering and monitoring
Copyright laws are not breached
Learners are taught to evaluate digital materials appropriately
Parents are aware of the acceptable use policy
Parents will be informed that all technology usage may be subject to monitoring, including website addresses and text
The school will take all reasonable precautions to ensure that users access only appropriate material
The school will audit use of technology to establish if the E-Safety policy is adequate and appropriately implemented
Methods to identify, assess and minimise risks will be reviewed annually
Complaints of internet misuse will be dealt with by a senior member of staff

I confirm that I have read, understood and will adhere to the above.

Trustee Name: _____

Signature: _____ Date: _____

Acceptable Use Policy for Community Users

This policy aims to ensure that community users of school digital technologies will be responsible users and stay safe while using these systems and devices. The policy is intended to protect school systems, devices and users from accidental or deliberate misuse that could put the security of the systems and users at risk.

I understand that:

I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school.

I understand that my use of school systems and devices and digital communications will be monitored.

I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.

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 that may cause harm or distress to others. I will not try to use any programs or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

I will immediately report any illegal, inappropriate or harmful material or incident; I become aware of, to the appropriate person.

I will not access, copy, remove or otherwise alter any other user's files, without permission.

I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.

I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.

I will not, without permission, 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 programs of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.

I will not disable or cause any damage to school equipment, or equipment belonging to others.

I will immediately report any damage or faults involving equipment or software, however this may have happened.

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 if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices and other technology access.

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.

Name: _____

Signature: _____ Date: _____