**Holy Family P.S.**

**Policy for**



**E-Safety**

Holy Family Primary School

E-safety policy

Holy Family Primary School recognises that ICT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. Using ICT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practice good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online.

E-safety covers the internet but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm children. There is a ‘duty of care’ for any persons working with children and educating all members of the school community on the risks and responsibilities of e-safety falls under this duty. It is important that there is a balance between controlling access to the internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in school, and provide a good understanding of appropriate ICT use that members of the school community can use as a reference for their conduct online outside of school hours. E-safety is a whole-school issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures which are outlined in our behaviour policy.

1. Roles and responsibility

The School e-Safety Coordinators are Mrs S Mullan (Junior Site)/ Mr Declan McCusker (Senior Site)

Signatures: .............................................................................................................

The designated member of the governing body responsible for e-safety is

………………………………………………….

Signature: ...............................................................................................................

2. Communicating school policy

This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used, and during PSHE lessons where personal safety, responsibility, and/or development are being discussed.

3. Making use of ICT and the internet in school

The internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school’s management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Some of the benefits of using ICT and the internet in schools are:

For students e.g.:

* Unlimited access to worldwide educational resources to support topics.
* Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
* Access to subject experts, role models, inspirational people and organisations.
* An enhanced curriculum with interactive learning tools; collaboration, locally, nationally, and globally.
* Self-evaluation; feedback and assessment
* Updates on current affairs as they happen.
* Access to learning whenever and wherever convenient.

For staff:

* Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
* Immediate professional and personal support through networks and associations.
* Improved access to technical support.
* Ability to provide immediate feedback to students and parents.
* Class management (SIMS)

For parents:

* Websites to support learning e.g. Seesaw, Study Ladder, Accelerated Reader, Mathletics.
* Accessing school information through email and the school website.

4. Learning to evaluate internet content

With so much information available online it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the school as part of digital literacy across all subjects in the curriculum. Students will be taught:

* to be critically aware of materials they read, and shown how to validate information before accepting it as accurate.
* to use age-appropriate tools to search for information online.
* to acknowledge the source of information used and to respect copyright.

The school will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of pupils. If staff or pupils discover unsuitable sites then the URL will be reported to the school e-safety coordinator. Any material found by members of the school community that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

5. Managing information systems

Classroom 2000 (C2k) is responsible for the provision of an information and communications technology (ICT) managed service to all schools in Northern Ireland. It provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.

Some of these safety services include:

* Providing all users with a unique user names and passwords
* Tracking and recording all online activity using the unique user names and passwords
* Scanning all C2k email and attachments for inappropriate content and viruses Filters access to web sites
* Providing appropriate curriculum software.

Should the school decide to access online services through service providers other than C2k then we will ensure that effective firewalls, filtering and software monitoring mechanisms are in place.

For more information on data protection in school please refer to our data protection policy. More information on protecting personal data can be found in section 11 of this policy.

6. Emails

The school uses email internally for staff and is an essential part of school communication. Staff should be aware that school email accounts should only be used for school-related matters, i.e. for staff to contact parents, other members of staff and other professionals for work purposes. This is important for confidentiality.

* Staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people and should not be accessed during school hours.
* Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications.
* Staff must a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
* The forwarding of chain messages is not permitted in school.

7. Published content and the school website

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, celebrating whole-school achievements and personal achievements, and promoting school projects. The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the school will be for the school office only. For information on the school policy on children’s photographs on the school website please refer to section 7.2 of this policy.

7.2 Policy and guidance of safe use of children’s photographs and work

Colour photographs and pupils work bring our school to life, showcase our student’s talents, and add interest to publications both online and in print that represent the school. However, the school acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Under the Data Protection Act 1998 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form. The school does this so as to prevent repeatedly asking parents for consent over the school year, which is time-consuming for both parents and the school. The terms of use of photographs never change, and so consenting to the use of photographs of your child over a period of time rather than a one-off incident does not affect what you are consenting to. This consent form will outline the school’s policy on the use of photographs of children, including:

* how and when the photographs will be used.
* how long parents are consenting the use of the images for
* school policy on the storage and deletion of photographs.

A template of the parents’ consent form can be found at the end of this policy.

Using photographs of individual children

The vast majority of people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using images, so we must ensure that we have some safeguards in place.

It is important that published images do not identify students or put them at risk of being identified. The school is careful to ensure that images published on the school website cannot be reused or manipulated through watermarking and browser restrictions. Only images created by or for the school will be used in public and children may not be approached or photographed while in school or doing school activities without the school’s permission. The school follows general rules on the use of photographs of individual children:

* Parental consent must be obtained. Consent will cover the use of images in: all school publications, on the school website, in newspapers as allowed by the school, in videos made by the school or in class for school projects.
* Electronic and paper images will be stored securely.
* Names of stored photographic files will not identify the child.
* Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that pupils are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the pupils.
* For public documents, including in newspapers, full names will not be published alongside images of the child.
* Groups may be referred to collectively by year group name.
* Events recorded by family members of the students such as school plays or sports days must be used for personal use only.
* Pupils are encouraged to tell a member staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
* Any photographers that are commissioned by the school will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the pupils.

*For more information on safeguarding in school please refer to our school child protection and safeguarding policy.*

7.3 Complaints of misuse of photographs or video

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our complaints policy for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools child protection and safeguarding policy and behaviour policy.

7.4 Social networking, social media and personal publishing

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. Pupils are not allowed to access social media sites in school. There are various restrictions on the use of these sites in school that apply to both students and staff.

Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHE about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school.

* Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways.
* They are all made fully aware of the school’s code of conduct regarding the use of ICT and technologies and behaviour online.
* Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
* The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately. • Safe and professional behaviour of staff online will be discussed at staff induction.

8. Mobile phones and personal device

While mobile phones and personal communication devices are commonplace in today’s society, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are:

* They can make pupils and staff more vulnerable to cyberbullying.
* They can be used to access inappropriate internet material.
* They can be a distraction in the classroom.
* They are valuable items that could be stolen, damaged, or lost.
* They can have integrated cameras, which can lead to child protection, bullying and data protection issues.

The school takes certain measures to ensure that mobile phones are used responsibly in school. Some of these are outlined below.

* The school will not tolerate cyberbullying against either pupils or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the school’s disciplinary sanctions read the school behaviour policy.

8.2 Mobile phone or personal device misuse

Pupils

* Pupils who breach school policy relating to the use of personal devices will be disciplined in line with the school’s behaviour policy. Their mobile phone may be confiscated.

Staff

* Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time.
* If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
* The school expects staff to lead by example. Personal mobile phones should be switched off or on ‘silent’ during school hours.

9. Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the behaviour policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the school will:

* Take it seriously: act as quickly as possible to establish the facts.
* Record and report the incident.
* Provide support and reassurance to the victim.
* Make it clear to the ‘bully’ that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the ‘bully’ will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school.

Repeated bullying may result in a fixed-term exclusion.

10. Managing emerging technologies

Technology is progressing rapidly and new technologies are emerging all the time. The school will risk-assess any new technologies before they are allowed in school, and will consider any educational benefits that they might have. The school keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

11. Protecting personal data

Holy Family Primary School believes that protecting the privacy of our staff and pupils and regulating their safety through data management, control and evaluation is vital to whole-school and individual progress. The school collects personal data from pupils, parents, and staff and processes it in order to support teaching and learning, monitor and report on pupil and teacher progress, and strengthen our pastoral provision.

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. Standardised Test results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

In line with the Data Protection Act 1998, and following principles of good practice when processing data, the school will:

* Ensure that data is fairly and lawfully processed.
* Process data only for limited purposes.
* Ensure that all data processed is adequate, relevant and not excessive.
* Ensure that data processed is accurate.
* Not keep data longer than is necessary.
* Process the data in accordance with the data subject's rights.
* Ensure that data is secure.
* Ensure that data is not transferred to other countries without adequate protection.

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

For more information on the school’s safeguards relating to data protection read the school’s data protection policy.

Signed by:

Chair of Governors……………………….………………………………. Date: ...............................

Principal ……………………….……………………………………………. Date: ..................................

Holy Family Primary School

Consent form for photographs and pupil work

Name of child ....................................... Date of birth ............................................

Name of parent ...............................................................

Holy Family Primary School believes that celebrating the achievement of children in school is an important part of their learning experience and personal development. Taking photographs and videos of pupils for internal display and displaying pupil work enables us to celebrate individual and group successes as a school community. We would also like to use photographs and videos of the school and its pupils to promote the good educational practice of the school. Children’s full names will never be published externally with their photographs, but may be published internally (for example, on display with their work).

**By signing this form you are consenting to the use of images of your child being used in the following outlets under the terms outlined in section 7 of our e-safety policy:**

**All school publications, on the school website, on the school social media outlets, in newspapers as allowed by the school, in videos made by the school or in class for school projects.**

**I consent /I do not consent to my child’s image being used in the above outlets.**

**Signed:………………………………………………… Date: ………………………………………………………**

**Please then return this form to your child’s class teacher by Friday 21st October.**

*N.B. This consent form covers consent for the duration of your child’s time at the school. Parents can withdraw or amend this consent at any time by notifying the school office in writing.*

*A full copy of the school’s policy on e-safety containing information on the safe use of photographs, videos, and the work of children in school can be found in the school office/on the school website. Go to* ***holyfamilyps.net***

**ICT Code of Safe Practice**

**(Pupils)**

**eSafety Rules**

* I will only use ICT in school for school purposes.
* I will not tell other people my ICT passwords.
* I will only open/delete my own files.
* I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
* I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
* I will not give out my own details such as my name, phone number or home address.
* I will not arrange to meet someone.
* I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
* I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.

**ICT Code of Safe Practice** **for Staff**

**eSafety Rules**

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to agree to this code of practice and adhere at all times to its contents. Any concerns or clarification should be discussed with Mrs. Sarah Mullan/Mr Declan Mc Cusker, school eSafety coordinators or Mrs. Maura Dolan (Principal)

* I will only use the school’s email / Internet / Intranet / Learning Platform and any related technologies for professional purposes.
* I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
* I will ensure that all electronic communications with staff are compatible with my professional role.
* I will only use the approved, C2k, secure e-mail system for any school business.
* I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Board of Governors. Personal or sensitive data taken off site must be encrypted.
* I will not install any hardware of software without permission of the ICT Coordinators.
* I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
* Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network.
* I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Principal.
* I will respect copyright and intellectual property rights.
* I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
* I will support and promote the school’s e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

***I agree to follow this code of practice and to support the safe and secure use of ICT throughout the school***

Signature …….………………….………………. Date ……………………

Full Name ……………………………………....(printed) Job Title . . . . . . . . . . . . . . . . .

Appendix 2

***Holy Family Primary School***

***Principal: Mrs.Maura Dolan***

***Junior School Senior School***

***Brook Street Brookmount Road***

***Omagh Omagh***

***Co-Tyrone BT78 5HD Co-Tyrone BT78 5HZ***

***Tel: 028 8224 4140 Tel: 028 8224 3551***

**Parental Agreement/Consent Letter**

Dear Parent/ Carer

As part of Holy Family Primary School’s Information and Communications Technology programme, we offer pupils supervised access to a *filtered* Internet service provided by C2k. Access to the Internet will enable pupils to explore and make appropriate use of many web sites that are of enormous educational benefit. They can also exchange messages with other Internet users throughout the world. However in spite of the tremendous learning potential, you should be advised that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

In order to help minimise any risks, which might arise from Internet use, our Service provider C2k has installed filtering software which operates by blocking thousands of inappropriate web sites and by barring inappropriate items, terms and searches in both the Internet and e-mail. To further enhance safety, pupils will only use the Internet for educational purposes, under the supervision of a member of staff.

The school’s rules for safe Internet use accompany this letter.   
Please read and discuss these with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mr. D. Mc Cusker (ICT Co-ordinator, Senior Site), Mrs. S. Mullan (ICT Co-ordinator, Junior Site), Mrs. S. McGuigan (V.P. Senior Site), Mrs. F. McGowan (V.P. Junior Site) or Mrs. M. Dolan (Principal).

**✂**

**Parent/ carer signature**

We have discussed this and ……………………………………..........(child’s name) agrees to follow the eSafety rules and to support the safe use of ICT at Holy Family Primary School.

Parent/ Carer Signature….…………………………………….……… Date………………………………………….

Appendix 3

**Sample Posters**

|  |  |  |
| --- | --- | --- |
| **Think then Click** | | |
| These rules help us to stay safe on the Internet | | |
|  | We only use the internet when an adult is with us |  |
|  | We can click on the buttons or links when we know what they do. |  |
|  | We can search the Internet with an adult. |  |
|  | We always ask if we get lost on the Internet. |  |
|  | We can send and open emails together. |  |
|  | We can write polite and friendly emails to people that we know. |  |

|  |
| --- |
| **Think then Click** |
| e-Safety Rules for Key Stage 2 |
| * We ask permission before using the Internet. * We only use websites that an adult has chosen. * We tell an adult if we see anything we are uncomfortable with. * We immediately close any webpage we not sure about. * We only e-mail people an adult has approved. * We send e-mails that are polite and friendly. * We never give out personal information or passwords. * We never arrange to meet anyone we don’t know. * We do not open e-mails sent by anyone we don’t know. * We do not use Internet chat rooms. |

**Principles for Internet Use ----- Children’s Version**

Be **SMART** On Line

|  |  |
| --- | --- |
| **S** | Secret Never give your address, telephone number, username or password when on-line. |
| **M** | **Meeting** someone or group you have contacted on-line is not allowed without the permission and supervision of your parent or teacher. |
| **A** | **Acceptin**g e-mails, opening sites or files requires the permission of your teacher, appointed adult or parent. |
| **R** | **Remembe**r no offensive language, text or pictures are to be displayed, sent, copied or received. |
| **T** | **Tell** your parent, teacher or trusted adult if someone or something makes you uncomfortable. |

# 

# Smile and Stay Safe Poster

**eSafety guidelines to be displayed throughout the school**

****

**and stay safe**

**S**taying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

**M**eeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

**I**nformation online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a ‘friend’

**L**et a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

**E**mails, downloads, messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

**Additional Advice for Parents with Internet Access at home**

1. A home computer with Internet access should be situated in a location where parents can monitor access to the Internet.
2. Parents should agree with their children suitable days/times for accessing the Internet.
3. Parents should discuss with their children the school rules for using the Internet and implement these at home. Parents and children should decide together when, how long and what constitutes appropriate use.
4. Parents should get to know the sites their children visit and talk to them about what they are learning.
5. Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available from Parents’ Information Network (address below).
6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities.
7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name or financial information such as credit card or bank details. In this way they can protect their children and themselves from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.
8. Parents should encourage their children not to respond to any unwelcome, unpleasant or abusive messages and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school they should immediately inform the school.

Further advice for parents is available from the following sources:

* <http://www.thinkuknow.co.uk>Thinkuknow - a mock cybercafé which uses online role-play to help children from 5 to 16+ explore a range of issues.
* <http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf> Aimed at parents and carers, there is a great deal of very clear information about chat rooms, social networking sites, email and much more.
* <http://www.parentscentre.gov.uk/usingcomputersandtheinternet> A very comprehensive site aimed at parents and carers. Includes many articles and external links to other helpful sites.
* <http://www.bbc.co.uk/webwise> Includes an ‘Internet for Beginners’ course and a tool for answering your internet related questions.
* <http://www.kidsmart.org.uk/> Explains the SMART rules for safe internet use and lots more besides.
* [http://www.ceop.gov.uk/](http://www.ceop.gov.uk) The government’s Child Exploitation and Online Protection Centre (CEOP)
* <http://www.parents.vodafone.com>Vodafone’s site is designed to help parents and carers develop an understanding of their child’s internet use.