Holy Family Primary School

E-Safety Policy

November 2018

Context

This policy is based on and complies with DENI Circular 2013/25 on 'eSafety Guidance'. It also complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools and DENI Circular 2011/22 and circular 2016/27 on Internet Safety. It will be reviewed annually.

This policy applies to all members of the School community who have access to and are users of the school ICT systems, both in and out of school. This includes pupils, staff including, all teaching and non-teaching staff, the Board of Governors, visitors, volunteers and other individuals who work for or provide services on behalf of the school.

This policy incorporates our Acceptable Use policy. It also must be read in conjunction with other relevant school policies including Data Protection policy, Child Protection policy, UICT policy, Anti-Bully policy and Behaviour policy.

This document sets out the policy and practices for the safe and effective use of the Internet and related technologies in Holy Family Primary School.

Rationale

Holy Family Primary School believes that e-safety is an essential element of safeguarding children and adults in the digital world when using technology.

We recognise that the internet and information communication technologies are now an important part of everyday life so children must be supported to be able to learn how to develop strategies to manage and respond to risk so they can be empowered to build resilience online.

Holy Family Primary School recognises its duty to provide the school community with quality internet access to raise educational standards, promote pupil achievement, support professional work of staff and enhance the schools management functions.

We identify a clear duty to ensure that children are protected from potential harm online.

Risks

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 and information technologies are powerful tools, which open up new opportunities for everyone. With these opportunities we also have to recognise the risks associated with the internet and related technologies.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face 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

Using the "Safeguarding Board for Northern Ireland (SBNI); Executive Summary – January 2014" we are able to further identify further risk and explore a variety of e-safety messages to our pupils, staff, parents and the wider school community. As highlighted in the report, these risks have been defined in various ways and are becoming more commonly categorised as follows:
Content risks: The child or young person is exposed to harmful material;
Contact risks: The child or young person participates in adult initiated online activity;
Conduct risks: The child or young person is a perpetrator or victim in peer-to-peer exchange;
Commercial risks: The child or young person is exposed to inappropriate commercial advertising, marketing schemes or hidden costs.

As with all other risks, it is impossible to eliminate the risk completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with any scenarios which may arise.

In Holy Family Primary School, we understand the responsibility to educate our pupils in e-Safety issues. We aim to teach pupils appropriate behaviours and critical thinking to enable them to remain both safe and legal when using the Internet and related technologies, in and beyond the context of the classroom.

Roles and Responsibilities

As e-Safety is an important aspect of Child Protection within the school, the Principal and Board of Governors have ultimate responsibility to ensure that the policy and

practices are embedded and monitored. It is the role of the ICT Co-ordinator to keep abreast of current e-Safety issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. The ICT Co-ordinator has responsibility for leading and monitoring the implementation of e -Safety throughout the school. The Principal/ICT Co-ordinator have the responsibility to update Senior Management and Governors with regard to e-Safety and all governors should have an understanding of the issues relevant to our school in relation to local and national guidelines and advice. The C2k Network provides robust filtering and security software. Monitoring reports of the use of this Network is available to the Principal/Network Manager on request.

E-Safety and Staff

- All staff will receive regular information and training on e-Safety issues through the Co-Ordinator at staff meetings. This includes information on DENI circulars regarding e-safety.
- All staff have an up to date awareness of e-safety matters and of the current school e-safety policy and practices.
- They are aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.
- All staff are expected to incorporate e-Safety into their activities and promote awareness within their lessons.
- Staff are aware of their responsibility to preview websites/online materials for use in their classroom prior to use.
- Staff are aware of the need to be vigilant when pupils are conducting investigative searches using search engines.
- All staff should take responsibility for the safety of pupil data/information including storage and use of images.
- All staff have read, understood and signed the school's Staff Acceptable Use Policy.
- New staff members will receive a copy of the e-Safety policy and Acceptable Use Agreement and sign an Acceptable Use Agreement.
- The Acceptable Use Agreement will also apply to external agencies/facilitators who, for reasons of staff training or presentation to pupils and parents, make use of the school's ICT equipment.
- Staff should be aware that all Internet traffic and email is monitored, recorded and tracked by the C2K system.

Handling of E-Safety Issues

Issues of Internet misuse and access to any inappropriate material by any user should be reported to the ICT Co-ordinator to be recorded in the E-Safety log. Issues of a child protection nature will be reported to the designated teacher and dealt with in accordance with the Holy Family Primary School Child Protection Policy.

Incidents of pupil misuse of technology which arise will be dealt with in accordance with the school's discipline policy.

E-safety and pupils

- e-safety will be discussed with pupils at the start of the year when they receive their Acceptable Use Agreement. This should be discussed as a set of rules that will keep everyone safe when using technology in school. Thereafter E Safety will be regularly discussed within the classroom to highlight its importance.
- Good practice guidelines for e-safety will be displayed in classrooms, around the school and in the ICT suite.
- Pupils will be informed that all network and Internet use is monitored.
- Pupils will participate in activities and/or assembly to raise awareness on Safer Internet Day
- They will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- They know and understand information within this policy in relation to the use of mobile phones, digital cameras and hand held devices. They also know and understand school policies on taking/using images and on cyberbullying.
- Pupils introduced to email are aware of the safety and 'netiquette' of using email both in school and at home.
- Pupils 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.

E-Safety and Parents

Holy Family Primary School will ensure that e-safety is promoted with parents/guardians. The e-Safety policy will be made available to parents with additional information leaflets and links posted on the school website and included in year group newsletters. Parents will be required to read the Acceptable Use Agreement for pupils and sign this agreement following discussion with their child.

The Internet

The Internet is a unique and exciting resource. It brings the world into the classroom by giving children access to a global network of educational resources. There is no doubt that the use of the Internet is an essential skill for children as they grow up in the modern world. The Internet is, however, an open communications' channel, available to all. Anyone can send messages, discuss ideas and publish materials with

little restriction. This brings young people into contact with people from all sectors of society and with a wide variety of materials, some of which could be unsuitable.

Networks

Pupil access to the Internet is through a filtered service provided by C2K, which should ensure educational use made of the resources is safe and secure, protecting users and systems from abuse. Parental permission is sought from parents before pupils access the Internet.

The C2K wireless network is also used with iPads in school. This network has appropriate filters applied for use by staff and pupils and use of iPads will only be carried out under staff supervision.

Connection of mobile phones or personal computers to the wireless network is not permitted.

Teaching and Learning

Internet use:

• The school will plan and provide opportunities within a range of curriculum areas to teach e-Safety.
• Educating pupils on the dangers of technologies that may be encountered outside school will be discussed with pupils through Safer Internet Day.
• Pupils will be made aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils will also be aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/guardian, teacher/trusted member of staff.
• The school Internet access is filtered through the C2k managed service.
• No filtering service is 100% effective; therefore, all children's use of the internet is supervised by an adult.
• Use of the internet is a planned activity. Aimless surfing is not encouraged. Children are taught to use the Internet in response to a need e.g. a question which has arisen from work in class.
• Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
• Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge, location, retrieval and evaluation.
• The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
• Children will be taught to be 'Internet Wise'. They will be made aware of Internet Safety Rules and encouraged to discuss how to cope if they come across inappropriate material.

E-mail: (where applicable)

• Pupils may only use C2k e-mail accounts on the school system.
• Pupils must immediately tell a teacher if they receive an offensive e-mail.

• Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
• The forwarding of chain mail is not permitted.
• Children will not always be given individual e-mail addresses. In some instances, children may have access to a group e-mail address to communicate with other children as part of a particular project. Messages sent and received in this way will be supervised by the teacher.

- Communication by e-mail between staff and parents should only be made using the c2k email account for the school. It should be professional and relate to school matters only.

- Individuals should not access the e-mail account of another individual within the school without express permission and a clear understanding of the reason for the proxy access.

School Website, Twitter and Home Seesaw

The Holy Family Primary School website, Twitter account and Home Seesaw promotes and provides up to date information about the school, as well as giving pupils an opportunity to showcase their work and other aspects of school life. In order to minimise risks of any images of pupils on the school website being used inappropriately the following steps are taken:

- Group photos are used where possible, with general labels/captions
- Names and images are kept separate – if a pupil is named their photograph is not used and vice-versa
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff

Social Networking:

- The school C2k system will block access to social networking sites.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. However, we accept that some pupils will still use them; they will be advised never to give out personal details of any kind, which may identify them or their location.
- Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Our pupils are asked to report any incidents of cyber-bullying to the school.
- School staff will not add children as 'friends' if they use these sites.

Password Security

- Adult users are provided with an individual login username and password, which they are encouraged to change periodically. Login details should not be shared with pupils.
- All pupils are provided with an individual login username and password.
- Pupils are only allowed to login using their own username and password.
- Pupils are not allowed to deliberately access files on the school network which belong to their peers, teachers or others.
- Staff Areas/Folders are the individual responsibility of each teacher to ensure they protect the security and confidentiality of the school network.
- Staff users must make sure that workstations/iPads are not left unattended and are locked.

Mobile Phones

Holy Family Primary School does not allow the use of mobile phones by children in school or on school trips.
The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety. In these instances the mobile phone must remain off during the school day. On occasion and when deemed necessary, the class teacher will take charge of the phone during the school day.

It is important to be aware of the safety issues regarding mobile phones which now increasingly have Internet access.

Staff use of mobile phones, only when necessary, should be discreet. Mobile phones should not be used in the classroom setting and should not be visible to pupils throughout school.

When on school outings, staff will be provided with a school mobile phone for contact with the school or in an emergency situation.

Use of Images, Video and Sound

It is recognised that many aspects of the Curriculum are enhanced by the use of multimedia. Staff and Pupils at Holy Family Primary School are encouraged to use iPads to create and use digital images, videos and sound recordings. They are taught to do so in a safe and responsible manner.

Digital images, video and sound recordings are only taken with the permission of the participants. Images and video are of appropriate activities and full names of participants are not used.

Parents/carers are required to sign an agreement regarding the taking and publishing of digital images of their children.

Staff or other visitors to Holy Family should never use a personal device – mobile phone, digital camera or other digital recording device to take photographs, video or sound recordings of the pupils.

Storage of Images

Digital and video images of pupils are always taken using school devices. Images are only permitted to be stored on a centralised area on the school network and are accessible to staff and to pupils under supervision. Photographs of pupils are generally removed when they leave school.

Cyberbullying

Cyberbullying can take many forms and guises including

- E-mail – nasty of abusive emails which may include viruses or inappropriate content
- Instant Messaging (IM) and Chat Rooms – potential to transmit threatening or abusive messages perhaps using a compromised or alias identity
- Social Networking Sites – typically includes the posting or publication of nasty or upsetting comments on another user's profile
- Online Gaming – abuse or harassment of someone using online multi-player gaming sites
- Mobile Phones – examples can include abusive texts, video or photo messages. Sexting can also occur in this category, where someone is encouraged to share intimate pictures or videos of themselves and these are subsequently transmitted to other people. Abusing Personal Information – may involve the posting of photos, personal information, fake comments and blogs, or pretending to be someone online without that person's permission.

Incidents of cyber-bullying will be dealt with in accordance with the School Anti-Bullying Policy.

Acceptable Use

Holy Family Primary School recognises the value the Internet and other digital information and communications technologies can add to the Learning and Teaching process. However we are also very aware of the risks associated with these technologies. We believe that all users should have an entitlement to safe Internet access at all times. As such, this Acceptable Use Policy is intended to ensure that:-

- All staff and pupils will be responsible users and stay safe while using the Internet and other communications
- All staff and pupils will adhere to Password security guidelines as stated in the e-safety policy
- All staff and pupils are familiar with acceptable and unacceptable internet use.
- Acceptable use of internet for both pupils and staff covers both fixed and mobile internet technologies provided by school as well as those owned by pupils and staff but brought onto school premises.
- All staff have read, understood and signed the school's Staff Acceptable Use Policy. *
- New staff members will receive a copy of the e-Safety policy and Acceptable Use Agreement and sign an Acceptable Use Agreement.*
- The Acceptable Use Agreement will also apply to external agencies/facilitators who, for reasons of staff training or presentation to pupils and parents, make use of the school's ICT equipment. *

*User Agreements available to C2k on request

Acceptable Use Agreement for Staff

The computer system is owned by the school and is made available to staff to enhance their professional activities including teaching, research, administration and management. The school's Internet Access Policy has been drawn up to protect all parties – the students, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

Staff should sign a copy of this Acceptable Internet Use Statement and return it to the Principal.

- All Internet activity should be appropriate to staff professional activity or the pupils' education
- Access should only be made via the authorised account and password, which should not be made available to any other person
- Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden
- Users are responsible for all e-mail sent and for contacts made that may result in e-mail being received
- Use for personal financial gain, gambling, political purposes or advertising is forbidden
- Copyright of materials must be respected
- Posting anonymous messages and forwarding chain letters is forbidden
- As e-mail can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material is forbidden

Name; _____

Signed; _____

Date; _____