Holy Family P.S

Growing in Faith and Love

Holy Family Primary School eSafety Policy

Version	Date	Revision Author	Summary of Changes	Review Date
Ver 1.0	17/5/17	S McQuaid	Ratified by Governors	May 2018
Ver 1.0	24/5/18	S McQuaid		May 2019
Ver 1.0	24/5/19	S McQuaid		May 2020
Ver 1.1	24/5/20	S McQuaid	Wireless provider changed. School website/Seesaw info updated.	May 2021
Ver 1.2	13/10/23	K McCallan	Updated references to social media and Addressing Bullying Policy	Oct 2026

This policy is based on and complies with DENI Circulars: 2007/1 Acceptable Use of the Internet and Digital Technologies in School; 2011/22 Internet Safety; 2013/25 eSafety Guidance; 216/26 Effective Uses of Mobile Digital Devices; and 2016/27 Online Safety.

Introduction

In Holy Family Primary and Nursery School we believe that the Internet and other digital technologies are very powerful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The Internet is an essential element of 21st century life for education, business and social interaction. This school provides pupils with opportunities to use the excellent resources on the Internet, along with developing the skills necessary to access, analyse and evaluate them.

The above circulars state that:

"Used well, digital technologies are powerful, worthwhile educational tools; technical safeguards can partly protect users, but education in safe, effective practices is a key goal for schools."

"Schools play a crucial role in raising awareness of the risks, highlighting the impact of behaviour when engaging with online technologies and educating children and young people about how to act appropriately and stay safe.

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

This policy has been drawn up by the staff of the school under the leadership of the Principal and the ICT coordinator.

It has been approved by governors and made available to all parents/guardians.

The policy and its implementation will be reviewed annually.

Code of Safe Practice

When using the Internet, email systems and digital technologies, all users must comply with all relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. The Code of Safe Practice for Holy Family Primary and Nursery School makes explicit to all users (staff and pupils) what is safe and acceptable and what is not.

The scope of the Code covers fixed and mobile Internet; school PCs, laptops, iPads and digital video equipment. It should also be noted that the use of devices owned personally by staff but brought onto school premises (such as mobile phones, iPads, tablets) is subject to the same requirements as technology provided by the school.

Wireless internet used for iPads is provided by C2K. It is password protected and subject to the same safe filtering system which is in place for accessing the internet on the C2K network. C2K Wireless is available in every classroom in the school.

The ICT Co-ordinator will monitor the effectiveness of the Code of Practice, particularly in the light of new developments in technology.

Code of Practice for pupils

Pupil access to the Internet on PCs and laptops is through a filtered service provided by C2K, which should ensure educational use of these resources is safe and secure, while protecting users and systems from abuse.

Parental permission is sought from parents before pupils access the internet.

The following key measures have been adopted by Holy Family Primary School to try to ensure that our pupils do not access any inappropriate material:

- Pupils using the internet will normally be working in highly-visible areas of the school;
- All online activity is for appropriate educational purposes and is supervised;
- Pupils will, where appropriate, use sites pre-selected by the teacher and appropriate to their age group;
- Pupils in Years 4-7 are educated in the safe and effective use of the internet, through a number of selected programmes.

It should be accepted, however, that however rigorous these measures may be, they can never be 100% effective. Neither the school nor C2K can accept liability under such circumstances.

The use of mobile phones by pupils is not permitted on the school premises during school hours, unless in exceptional circumstances, where permission may be granted by a member of staff. If a pupil needs to bring a mobile phone to school for use after school, a consent form must be completed by a parent and the phone kept in a locked drawer in the school office throughout the day.

During school hours pupils are forbidden to play computer games or access social networking sites, unless specifically assigned by the teacher.

Networking sites, besides ‘MySchool’, which is filtered and monitored by C2k, are not accessible for pupils.

Google Apps are available for all pupils, with accounts set up using C2K usernames, which should only be used for school related material.

Sanctions

Incidents of technology misuse which arise will be dealt with in accordance with the school’s discipline policy. Minor incidents will be dealt with by the Principal/ICT Co-ordinator and may result in a temporary or permanent ban on Internet use.

Incidents involving child protection issues will be dealt with in accordance with school child protection procedures.

Code of practice for staff

Staff have agreed to the following Code of Safe Practice:

- Pupils accessing the internet should be supervised by an adult at all times;
- All pupils are aware of the rules for the safe and effective use of the internet. These are displayed in classrooms and discussed with pupils;
- All pupils using the internet have written permission from their parents;
- Recommended websites for each year group are available under *Favourites*. Any additional websites used by pupils should be checked beforehand by teachers to ensure there is no unsuitable content and that material is age-appropriate;
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/I.C.T. Co-ordinator;
- In the interests of system security, staff passwords should only be shared with the network manager;
- Teachers are aware that the C2K system tracks all pupil internet use and records the sites visited;
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these;
- Photographs of pupils should, where possible, be taken with a school camera/iPad and images stored on a centralised area on the school network/password protected internet storage, accessible only to teaching staff.
- Teacher iPads must be passcode protected.
- School systems may not be used for unauthorised commercial transactions.

Internet Safety Awareness

In Holy Family Primary and Nursery School we believe that, alongside having a written e-safety policy and code of practice, it is essential to educate all users in the safe and effective use of the Internet and other forms of digital communication. We see the educational use of the internet as an appropriate, effective, safe and essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

Internet Safety Awareness for pupils

Rules for the acceptable use of the internet are discussed with all pupils. Pupils across the school follow a structured programme of Internet Safety Awareness and Digital Literacy in PDMU using a range of online resources:

www.childnet.com

www.bbc.co.uk/cbbc/topics/stay-safe

www.thinkuknow.co.uk/

www.saferinternet.org.uk

www.commonsense.org

In addition, pupils in Key Stage 2 revisit the importance of appropriate online behaviour through the NSPCC Keeping Safe programme.

Internet Safety Awareness for staff

The ICT Co-ordinator will keep staff informed and updated on issues relating to internet Safety and attend courses when available. This training will then be disseminated to all teaching staff, classroom assistants and supervisory assistants on a regular basis.

Internet Safety Awareness for parents

The esafety and acceptable use of the internet and digital technologies policy and Code of practice for pupils is available for parents. Internet safety leaflets for parents and carers may need to be sent home when necessary. Parent awareness evenings are organised and facilitated by external agencies where appropriate.

Community Use of School ICT Resources

Where the school's ICT facilities are used as a community resource under the Extended Schools programme, users are issued with temporary usernames and passwords by C2K. They must also agree to the school's Acceptable Use of the Internet policy before participating and only access pre-selected and appropriate websites under the guidance of a tutor.

Health and Safety

Holy Family Primary School has attempted, so far as is possible, to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and in the resource areas, which has been designed in accordance with health and safety guidelines. Pupils are supervised at all times when using digital technology.

Digital and Video Images of Pupils

Parental permission, in writing, is sought at the beginning of each school year to cover the use of photographs of pupils on the school website; the school Facebook page; Seesaw journals; in the local press; and for displays within school. It is the parent's responsibility to inform the school of any changes in permission with regard to digital images.

Storage of images

Digital and video images of pupils are, where possible, taken with school equipment. Images are stored on a centralised area on the school network. Images may also be shared with the website co-ordinator through staff Google Drive accounts, which are password protected.

School Website

Our school website (www.holyfamilypsbelfast.org.uk) and Facebook page (www.facebook.com/holyfamilyprimaryschoolbelfast) promote and provide 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 or Facebook page being used inappropriately the following steps are taken:

- Group photos are used where possible, with general labels/captions;
- Names and images are kept separate;
- The website does not include home addresses, telephone numbers, personal e-mails or any other personal information about pupils or staff.

Seesaw

Seesaw is a digital learning journal which is also used for home-school communication. Children can use their Seesaw journal to share their learning from home and in school. At times, this includes photos and videos of children. Seesaw accounts have been set up so that children and parents cannot see the journals of other children. Parents may be able to see group photos of other children on their child's journal.

Social Software

Chatrooms, blogs and other social networking sites are blocked by the C2K Network and Wirelass filters, so pupils do not have access to them in the school environment. Such communication is maintained within the educational learning environment on the C2K system (My School). Pupils are discouraged from joining age inappropriate social networking websites outside of school, eg. Facebook, Instagram, Snapchat.

However, we regard the education of pupils on the safe and responsible use of social communication software as vitally important and this is addressed through our Internet Safety Education for pupils.

Instances of cyber bullying of pupils or staff will be regarded as very serious offences and dealt with according to the school‘s Addressing Bullying policy and Safeguarding procedures. Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

Staff Code of Conduct for Use of Internet and Digital Technology

- Pupils accessing the Internet should supervised by an adult at all times;
- All pupils are aware of the rules for the safe and effective use of the internet. These are displayed in classrooms and discussed with pupils;
- All pupils using the internet have written permission from their parents;
- Recommended websites for each year group are available under *Favourites*. Any additional websites used by pupils should be checked beforehand by teachers to ensure there is no unsuitable content and that material is age-appropriate;
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the Principal/ICT Co-ordinator;
- In the interests of system security, staff passwords should only be shared with the network manager;
- Teachers should be aware of copyright and intellectual property rights and should be careful not to download or use any materials which are in breach of these;
- Photographs of pupils should, where possible, be taken with a school camera/iPad and images stored on a centralised area on the school network/password protected internet storage, accessible only to teaching staff.
- Teacher iPads must be passcode protected.
- School systems may not be used for unauthorised commercial transactions.

Staff Code of Conduct for Social Networking

- Individuals who work with children and young people, should exercise caution when using social networking sites and avoid inappropriate communication of any kind.
- Staff should always maintain appropriate professional boundaries when online, avoid improper contact or relationships and respect their position of trust.
- With regard to relationships, staff should not attempt to establish an inappropriate relationship which might include: communication of a personal nature; inappropriate dialogue through the internet; or sending emails or text messages of an inappropriate nature
- Staff relationships with children and young people should at all times remain professional and they should **not** correspond with children and young people through such sites or add them as 'friends'.
- Staff should take care as to the information they display about themselves and their personal lives online.
- Staff should also ensure that they have installed and are using the appropriate privacy settings for each social networking site they use.
- Individuals who work with children and young people, should NEVER make, view or access illegal or inappropriate images of children.

Signed:_________________________________ Date:______________________