



E-Safety Policy

Reviewed January 2021

Context

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and Digital Technologies in Schools and DENI Circular 2011/22 on Internet Safety.

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."

This document sets out the policy and practices for the safe and effective use of the Internet and related technologies in Sacred Heart P.S.

Care and responsibility

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

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 Sacred Heart P.S., 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.

E-Safety Skills Development for Staff

- All staff will receive regular information and training on E-Safety issues through the Co-Ordinator at staff meetings.
- All staff have been made 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.
- New staff members will receive a copy of the E-Safety policy and Acceptable Use Agreement and sign an Acceptable Use Agreement.
- All staff are encouraged to incorporate E-Safety into their activities and promote awareness within their lessons.

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 Sacred Heart P.S. 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.

Activities throughout the school year including Internet Safety Day will refresh E-Safety and further pupils' understanding.

Pupils will be informed that all network and Internet use is monitored.

E-Safety and Parents

The Sacred Heart P.S. E-Safety policy will be published on the school website and parents will be encouraged to read the document. Parents will be required to read the Acceptable Use Agreement for pupils and sign this agreement following discussion with their child.

Sacred Heart P.S. will look to promote E-Safety awareness within the school community which may take the form of parents' information evenings, information leaflets or links on the school website.

E-Safety and Staff

All staff will be introduced to the E-Safety policy and its importance explained. Staff will be asked to read and sign the Acceptable Use Agreement for Staff which focuses on E-Safety responsibilities in accordance with the Code of Conduct for employees set out in the Staff Handbook.

Staff should be aware that all Internet traffic and email is monitored, recorded and tracked by the C2K system.

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.

Connection of mobile phones or personal computers to the wireless network is restricted by secure password. Access will be granted after consideration by Principal/ICT Coordinator.

Learning and Teaching

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 Key Stage 2 pupils through Internet Awareness 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:

- 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.

School Website/ Social Media

The Sacred Heart P.S. website 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 unless prior permission is given by parent.
- 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 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.
- Permission should not be given to allow members of staff or substitute teachers access to accounts other than their own. Substitute teacher accounts exist for temporary purposes.

Mobile Phones

Sacred Heart P.S. does not allow the use of mobile phones by children in school or on school trips.

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.



Internet Safety Pledge (P1 – P3)

Place a ✓ in each box after you've read it carefully. Sign the bottom to agree to the pledge and return it to your teacher.

- ☐ I promise to never send or post personal information, such as my addresses, phone number, or school name.
- ☐ I will never send a picture of myself to anyone without a parent's permission.
- ☐ I will not open e-mails from people I don't know.
- ☐ I will not follow links to sites that I do not recognize.
- ☐ I will tell an adult if I see any information on the Internet that makes me feel uncomfortable.
- ☐ I will never give out my passwords to anyone, except my parents.
- ☐ I will never download and install files to my computer without a parent's permission.
- ☐ I will never e-mail or post mean or hurtful things about other people.
- ☐ I will follow all Internet rules set by my school and my parents.

Using the Internet is a special privilege for responsible people. I promise to be safe online.

Signature of Pupil

Signature of Parent/Guardian

Date





Acceptable Use of the Internet (P4-7)

Children should know that they are responsible for their use of the Internet in school and that they do so in a safe and appropriate manner.

Please discuss these guidelines with your child and stress the importance of safe use of the Internet.

Pupils:

- On the network, I will only use my own login username and password
- I will keep my username and password private
- I will not access other people's files without their permission
- I will not change or delete other people's work/files
- I will ask permission before entering any website, unless my teacher has already approved that site
- I will use the Internet for research and school purposes only
- I will only send e-mail in school when directed by the teacher as part of ICT lessons. I will make sure that the messages I send are polite and responsible
- I understand that the use of strong language, swearing or aggressive behaviour is not allowed when using online forums etc
- When commenting online I will not give my name, address or phone number or arrange to meet anyone
- I understand that I am not allowed to enter Internet Chat Rooms or Social Media while in school
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately
- I will not bring in memory sticks etc from home to use in school unless I have been given permission by my class teacher
- I understand that the school may check my computer files/Emails and may monitor the Internet sites that I visit
- I understand that if I deliberately break these rules I could be stopped from using the Internet and my Parent/Guardian will be informed

Signature of Pupil

Signature of Parent/Guardian

Date





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
- Permission should not be given to allow members of staff or substitute teachers access to accounts other than their own. Substitute teacher accounts exist for temporary purposes.

Signed _____

Date _____