

Acceptable Use of the Internet & Digital Technology Policy

This policy is based on and complies with DENI Circular 2007/1 on Acceptable Use of the Internet and digital Technologies in Schools

Introduction

In St. Joseph's Primary School we believe that the Internet and other digital technologies are very powerful resources which can enhance and potentially transform learning and teaching 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 in a safe, responsible manner.

The above circular states 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 safe and effective use of the internet in St. Joseph's Primary School. The policy has been drawn up by the ICT Coordinator and Principal. It has been approved by governors and is available to all parents. The policy and its implementation will be reviewed bi-annually.

Code of Safe Practice

When using the internet, e-mail 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 St. Joseph's Primary 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 PC's, laptops and digital video equipment. It should also be noted that the use of devices owned personally by staff and pupils but brought onto school premises (such as mobile phones, laptops, etc) are subject to the same requirements as technology provided by 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 is through a filtered service provided by C2K, which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse. Parental permission is sought from parents on an annual basis before pupils access the Internet.

In addition, the following key measures have been adopted by St. Joseph's to ensure our pupils do not access any inappropriate material:

- The school's Code of Practice for use of the Internet and other digital technologies (enclosed) is made explicit to all pupils.
- 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 possible, use sites pre-selected by the teacher and appropriate to their age group.
- Pupils in Key Stage 2 are educated in the safe and effective use of the Internet, through a number of selected programmes. (Think U Know, 360, etc)

It should be accepted, however, that as rigorous as 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 the class teacher or Principal/Vice Principal and the mobile phone placed securely in the office for safe keeping.

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 adhere 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 the ICT room and discussed with pupils.
- All pupils using the Internet have written permission from their parents.
- 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 are aware that the C2K system tracks all Internet use and records the sites visited. The system also logs emails and messages sent and received by individual users.
- 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 and images should be stored on a centralised area on the school network, accessible only to teaching staff.
- School systems may not be used for unauthorised commercial transactions.

Internet Safety Awareness

In St. Joseph's we believe that, alongside having a written 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 education in appropriate, effective and safe use as an essential element of the school curriculum. This education is as important for staff and parents as it is for pupils.

What are the Dangers?

The Internet is 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.

Internet Safety Awareness for pupils

Rules for the Acceptable use of the Internet are discussed with all pupils and are displayed. In addition, Key Stage 2 pupils follow a structured programme of Internet Safety Awareness using a range of online resources. Eg. CEOP, Think You Know programmes. All children also participate in Internet Safety Day each year and revisit safety websites.

Internet Safety Awareness for Staff

The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety and attends regular courses. This training is then disseminated to all teaching staff, classroom assistants and supervisory assistants on a regular basis.

Points for teachers to consider:

- Internet use should be planned, task orientated and educational within a regulated and managed environment.
- *Supervision is the key strategy.* Children should have a teacher or classroom assistant present when using the Internet. Computers should be positioned so that it is possible for adults to see materials on screen.
- Children should know why they are using the Internet. Teach children to use the Internet in response to a need. E.g. to answer a question which has arisen from work in class.
- Search engines require careful use and planning/supervision. Children can be bombarded with information and yet fail to find the material they need.
- Children do not need thousands of website addresses. A small appropriate choice is much more effective.
- Individual e-mail addresses may not be considered appropriate for younger children. Fronter and/or Equella should be used for whole class projects/homeworks.
- Discuss with pupils the rules for responsible Internet use. It is not enough to protect children from materials, we must teach them to become Internet Wise.
- Children need to learn to recognise and avoid the risks.
- Children need to know what to do if they come across inappropriate material or if they are approached by a stranger.

C2K Internet Filtering

C2K filtering includes three internet security groups to which schools can add users to allow access to additional sites. Access to these groups is at the discretion of the Principal alongside the ICT Co-ordinator and requests from class teachers.

The three groups are:

Internet Advanced: This group contains a number of sites that were previously accessible by all users in primary schools (eg. webmail, shopping, sex education and lifestyle sites). As such, you may wish to consider adding all staff to this security group in order to facilitate a smooth transition.

Internet Social Networking: This group contains Twitter, Facebook, LinkedIn and Wordpress.

Internet Streaming Media: This group contains YouTube, Vimeo, BBC iPlayer and other mainstream video streaming sites

(As a number of websites are no longer supported on Internet Explorer 7, schools are advised to use Google Chrome browser where possible. Please note, this transfer will also address the Google search issue that has been on-going with Chrome.)

Health and Safety

St. Joseph's have attempted, in so far as possible, to ensure a safe working environment for pupils and teachers using ICT resources, both in classrooms and in the ICT suite, which has been designed in accordance with health and safety guidelines. Pupils are supervised at all times when Interactive Whiteboards and ICT equipment are being used.

Digital and Video Images of Pupils

See 'Policy for the Use of Photography & Videos'.

Social Software

See 'Social Networking Policy'.

Policy Review

Internet technology and school use of resources will develop and change with time. It is our responsibility to revise and up-date our Internet Safety Policy as appropriate and where necessary.

