Acceptable Use of the Internet and Digital Technology Policy



St Brigid’s PS Mayogall

Ratified by Board of Governors on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signed : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**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 Brigid’s, 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. Our 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.”

**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 Brigid’s 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, iPads, laptops, chromebooks 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, camera phones, PDAs) is 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 currently 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. A second line was installed within the school as part of our telephone contract with Standard Utilities. This was to facilitate for the use of our 120 chromebooks used in the JDO Project. A new upgraded c2kwireless network will be installed in school in the first term of 22/ 23 school year.

Parental permission is sought from parents on child’s enrolment before pupils access the Internet.

Both parties sign this ICT Code of Practice Agreement and copies of these are held on file by the ICT Co-ordinator. In addition, the following key measures have been adopted by St. Brigid’s PS 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 is made explicit to all pupils and is displayed prominently;

Our Code of Practice is reviewed each school year and signed by pupils/parents;

Pupils using the Internet will 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; All pupils learn about internet safety as part of PDMU. 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.

Mobile Phones

The use of mobile phones by pupils is not normally permitted on the school premises during school hours, unless in exceptional circumstances.

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

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 prominent locations within the school and discussed with pupils.

All pupils using the Internet have written permission from their parents.

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.

Staff 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, be taken with a school iPad/camera and images should be stored on the school network, accessible only to teaching staff.

School systems may not be used for unauthorised commercial transactions.

Internet Safety Awareness

In St. Oliver Plunkett PS 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 of the internet 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.

Key Concerns are:

## Potential Contact

Children may come into contact with someone online who may wish to harm them. Some adults use chat rooms or e-mail to communicate with children for inappropriate reasons.

Children need to be taught:

* That people are not always who they say they are.
* That “Stranger Danger” applies to the people they encounter through the Internet.
* That they should never give out personal details or
* That they should never meet alone anyone contacted via the Internet

## Inappropriate Content

Through the Internet there are unsuitable materials in many varieties. Anyone can post material on the Internet. Some material is published for an adult audience and is unsuitable for children e.g, materials with a sexual content. Materials may express extreme views, such as information on weapons, crime and racism which would be restricted elsewhere. Materials may contain misleading and inaccurate information. E.g., some use the web to promote activities which are harmful such as anorexia or bulimia.

Children need to be taught:

* That information on the Internet is not always accurate or true.
* To question the source of information.
* How to respond to unsuitable materials or requests and that they should tell a teacher/adult immediately.

## Internet Safety Awareness for pupils

Rules for the Acceptable use of the Internet are discussed with all pupils and are prominently displayed in prominent areas in the school. In addition, Pupils learn about Online Safety through PDMU lessons at all age groups in school. A wide variety of resources are used. For example

NSPCC Keeping Safe

Digiduck Stories, SMART activities, Smartie the Penguin - Childnet International

Think You Know – CEOP

C2K Newsdesk

PSNI Cyber Safety Talk

## Internet Safety Awareness for parents

The Online Safety Policy is available for parents by request and is also posted on the

 school website. The Code of practice for pupils is sent home at the start of each school year (Via Google Forms) for parental digital signature. Internet safety leaflets for parents and carers are also sent home biannually.

 .

## Digital and Video Images of Pupils

Parental permission is sought at the start of each school year to cover the use of photographs of pupils on the school website, in the local press and for displays etc within school and written permission must be obtained from the parent/carer.

## School Website

Our school website aims to 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. To minimize risks of images being used inappropriately we;

* Keep names and images seperate– if a pupil is named their photograph is not used and vice versa;
* The website does not include home addresses, telephone numbers, personal emails or any other personal information about pupils or staff.
* Website links selected by teachers may be put on the website for pupils to access outside of school – sites will be previewed and checked regularly. Parents’/Carers’ permission will be sought to publish pupils work and/or photographs. These will only be published subject to the strict safeguards above.

## Storage of images

Digital and video images of pupils are, taken with school equipment. Images are stored on the school network accessible only to teaching staff. Photographs taken using class ipads are used, uploaded to the school google Drives or deleted.

## Social Software

Chatrooms, blogs and other social networking sites are blocked by the C2K filters so pupils do not have access to them in the school environment. However, we regard the education of pupils on the safe and responsible use of social 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 discipline policy and child protection procedures.

Pupils are aware that any misuse of mobile phones/websites/email should be reported to a member of staff immediately.

All reasonable and appropriate steps have been taken to protect pupils. The school recognises that despite employing safety procedures, in some circumstances, the Internet may give children access to undesirable information or images. Children are regularly reminded that should they encounter inappropriate material on line they must immediately leave that website Inform an adult

Should a child or teacher encounter unsuitable material through the managed service, this will be reported to C2k via the C2k helpdesk number.

## Policy Review

Internet technology and school use of resources will develop and change with time. At St Brigid’s we aim to revise and up-date our Accceptable Use Policy as appropriate and where necessary.