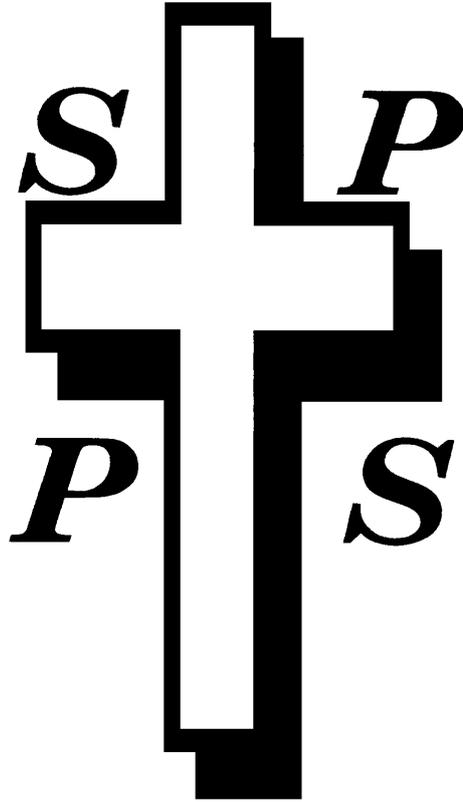


# St Patrick's PS



## Internet/E-Safety Policy

Review due: Feb 2024

## **Introduction**

This policy is based on and complies with DENI Circulars 2007/1, 2011/22 and 2013/25 on Acceptable Use of the Internet and Digital Technologies in Schools.

In St Patrick's P.S we believe that the internet and other digital technologies are very useful resources which can enhance and potentially transform teaching and learning when used effectively and appropriately. The internet is an essential element of the 21<sup>st</sup> century life for education, business and social interaction. St Patrick's P.S provides pupils and staff with opportunities to use the excellent resources on the internet, along with developing the skills necessary to access and evaluate them.

Whilst these ICT resources can be exciting and beneficial both in and out of the context of education, all users need to be aware of the range of risks associated with the use of Internet Technologies.

In St Patrick's P.S we understand the responsibility to educate our pupils in e-Safety issues. We aim to teach our children 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.

This policy sets out the policy and practices for safe and effective use of the internet in St Patrick's P.S

The policy and its implementation will be reviewed biannually.

## **Code of Safe Practice.**

When using the internet, email system and digital technologies, all users must comply with all the relevant legislation on copyright, property theft, libel, fraud, discrimination and obscenity. The Code of Safe Practice for St Patrick's P.S makes it clear to all users, staff and pupils what is safe and acceptable and what is not.

The Code covers fixed and mobile internet, school PCs, laptops and digital video equipment. It should be noted that the use of devices owned personally by staff and pupils but brought into school premises 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.

## **Code of Safe Practice for Pupils.**

Pupils access to the internet is through a filtered service provided by C2K, which ensures 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 Patrick's P.S to ensure our pupils do not access inappropriate material:

- The school's Code of Practice for use of the Internet and other digital technologies is made clear to all pupils and is shared with parents annually.
- Our Code of Practice is reviewed annually.
- Pupils using the internet will be working in highly visible, communal areas.
- All online activity is for appropriate educational purposes and is supervised.
- Pupils will where possible use sites pre-selected by the teacher/staff and appropriate to their age.
- Pupils are educated in the safe and effective use of the internet, through a number of selected programmes.

It should be accepted, 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/Computer Games**

Refer to Mobile Phone Policy

## **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 and may result in a temporary 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 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.

Rules for safe use of the internet are broadly speaking similar to the ones listed below, however they may change slightly from year to year as they are formulated at the start of each year by the children themselves in each class.

Staff must ensure that pupils know and understand that no Internet user is permitted to:

- ❖ retrieve, send, copy or display offensive messages or pictures;
- ❖ use obscene or racist language;
- ❖ harass, insult or attack others;

- ❖ damage computers, computer systems or computer networks;
  - ❖ violate copyright laws;
  - ❖ use another user's password;
  - ❖ trespass in another user's folders, work or files;
  - ❖ intentionally waste resources (such as on-line time and consumables);
  - ❖ use the network for unapproved commercial purposes.
- Deliberate/accidental access to inappropriate materials or any other breaches of the school code of practice should be reported immediately to the principal or Mr McGlone, the designated Child protection teacher.
  - 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 the 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 the school network, accessible to staff and pupils under supervision.
  - School systems may not be used for unauthorised commercial transactions.

### **Internet Safety Awareness**

In St Patrick's P.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. The UICT co-ordinator is aware of the Child exploitation and Online Protection (CEOP) website with access to all available teaching resources. [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) Other useful websites used for upskilling parents and staff as well as educating children include [www.childnet.com](http://www.childnet.com) [www.nspcc.org.uk](http://www.nspcc.org.uk)

### **Internet Safety Awareness for Pupils.**

Rules for the acceptable use of the Internet are discussed with all pupils and are displayed in classrooms.

### **Internet Safety Awareness for Staff.**

The ICT Co-ordinator keeps informed and updated on issues relating to Internet Safety and will attend courses if available. This training is disseminated to all staff.

### **Internet Safety Awareness for Parents.**

The Internet Safety Agreement for pupils is sent home at the start of each school year for parental signature. Pupils are also made aware of the UICT Code of Practice in our school. PSNI Internet Safety Presentations are publicised and facilitated in school. The school website, monthly newsletters and school text service make parents/carers aware of where to read the school's updated UICT and eSafety policies as well as informing them of relevant eSafety awareness evenings being presented.

## Advice for Parents

- While in school, teachers will guide pupils toward appropriate materials on the internet. Outside school, parents or guardians bear the same responsibility for such guidance as they would normally exercise with information sources such as television, telephones, movies, Ipads, smartphones and other media.
- Appropriate home use of the internet by children can be educationally beneficial, and can make a useful contribution to home and schoolwork. However, we advise parents that this use should be supervised. Parents should be aware that they are responsible for their children's use of internet resources at home.

Our advice to parents is that it is good practice to provide filtered and monitored access to the internet for your children. We ask you to consider the following guidance and advice on its use that you might find helpful at home.

Parents should:

- ✓ discuss with their children the rules for using the Internet and decide together when, how long, and what comprises appropriate use;
- ✓ get to know the sites their children visit, and talk to them about what they are learning;
- ✓ ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name, or financial
- ✓ explain to the children information such as credit card or bank details. In this way they can protect their children (and themselves) from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud;
- ✓ encourage their children not to respond to any unwelcome, unpleasant or abusive messages, and to tell them if they receive any such messages or images. If the message comes from an Internet service connection provided by the school, they should immediately inform the school.

Please note that nowadays there are a lot of social communication sites where people can communicate with their peers. Sites such as Facebook, Twitter, Snapchat, Instagram are not suitable for primary aged children and in fact most of these sites are age restricted. A lot of the content and conversations on these sites are inappropriate for young children. We advise parents to monitor which sites your children are visiting at home. Advice to parents on how to deal with use of social media by pupils is contained in our social media policy. Basically if offensive/inappropriate material is posted by a pupil of our school, it should be reported to the host of the social media website and/or reported to PSNI.

St Patrick's P.S parents can be assured that their children are only using the Internet in school for educational reasons. Educational games nowadays are so advanced that pupils are enjoying a useful learning experience. Nevertheless, should your child report any seemingly inappropriate materials on the computers, please contact us immediately and we shall look into the matter if it is within our jurisdiction. All users must be aware that their use of the Internet is monitored and that action will be taken to counter any abuse.

## **Health and Safety**

St Patrick's P.S have attempted in so far as possible, to ensure a safe working environment for pupils and teachers while using ICT resources in classrooms. Pupils are supervised at all times when using UICT equipment.

## **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 monitor, in local press and for displays etc, written permission must be obtained from parent/carer.

## **Storage of images**

Digital and video images of pupils, where possible, are taken with school equipment. Images should only be stored and accessed through the school network.

## **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. Children will under very strict supervision be permitted to use frontier.

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 Policy 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 procedures.

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

## **Cyber Bullying and the link to Anti Bullying Policy**

Staff and Parents should be aware that pupils may be subject to cyber bullying via electronic methods of communication both in and out of school. This form of bullying is considered within the school's Anti -Bullying policy and pastoral services as well as here in the E-Safety Policy.

In St Patrick's PS we do not endorse the use of social media for teaching and learning as although it can offer much to schools and pupils, it also brings its own unique issues and concerns.

Cyber Bullying can take many different forms and guises including:

- Email – nasty or 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.

Whilst cyber-bullying may appear to provide anonymity for the bully, most messages can be traced back to their creator and pupils should be reminded that cyber-bullying can constitute a criminal offence. While there is no specific legislation for cyber-bullying, the following may cover different elements of cyber-bullying behaviour:

- Protection from Harassment (NI) Order 1997  
<http://www.legislation.gov.uk/nisi/1997/1180>
- Malicious Communications (NI) Order 1988  
<http://www.legislation.gov.uk/nisi/1988/1849>
- The Communications Act 2003  
<http://www.legislation.gov.uk/ukpga/2003/21>
- Addressing Bullying in Schools Act (Northern Ireland) 2016  
<https://www.legislation.gov.uk/nia/2016/25/contents/enacted>

Pupils will be encouraged to report incidents of cyber-bullying to the social media website provider and, if appropriate, the PSNI to ensure the matter is properly addressed and the behaviour ceases. Cases of cyber-bullying that occur in school will be recorded as with other behaviour incidents through the Anti-Bullying Policy.

## E-Safety

Dear Parent

At St Patrick's Primary School, we recognise the use of ICT and communications facilities as an important resource for teaching and learning. However, at all times users will encounter risks, posed more by behaviours and values online than the technology itself. Consequently, during ICT and other lessons in which ICT is used, we will ensure that they are taught and made aware of appropriate safe and responsible online behaviours to safeguard themselves and get the most of the technology itself.

Please read the rules over the page with your child and then sign and return the page asap or by Wednesday 23<sup>rd</sup> November.

In the event of a breach of Rules by any child, the parent will be informed and the pupils may have the privilege withdrawn.

These Rules provide an opportunity for further conversations between you and your child about safe and appropriate use of the Internet and other on-line tools (eg mobile phone), both within and beyond school.

Please contact myself should you wish to discuss the matter further.

Yours sincerely,

***P Torney***

Principal

### **e-Safety Agreement - 2022/2023**

**Does your child have access to a computer**                      **yes / no**

**Does your computer have internet access**                      **yes / no**

**Pupil / Parent agreement:**

- We have read and discussed the Rules and confirm that we have understood what they mean.

Pupil signature \_\_\_\_\_ Class \_\_\_\_\_

Parent signature \_\_\_\_\_ Date \_\_\_\_\_

## Key Stage 2

**These are our Rules for using the internet safely and responsibly.**

- We will use the internet to help us learn and we will learn how to use the internet safely and responsibly.
- We will ask permission from a member of staff before using a computer and accessing the internet.
- We send emails and phone messages that are polite and friendly.
- We only use our school email address in school during lessons, with permission from a member of staff.
- We only e-mail/message people an adult has approved.
- Adults are aware when we use on-line tools and have given permission.
- We only access systems with our own username.
- We do not access other people's files
- We never give out or share passwords or personal information (like our surname, address or phone number).
- We do not bring in data storage devices e.g. memory sticks from outside school unless we have permission from a teacher.
- We never post photographs or video clips without permission and never include surnames with photographs.
- If we need help we ask a teacher or adult.
- If we see anything on the internet or in an email that makes us uncomfortable, we will immediately inform a teacher or parent.
- If we receive a message sent by someone we don't know we know we will not reply and alert the teacher or parent immediately.
- **We do not bring mobile phones into school.**
- We will report any mobile phones seen in school to a member of staff.
- We know that we should follow the rules as part of the agreement with our parent.
- We are able to look after each other by using our safe internet in a responsible way.
- We know that we can go to [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk) for help.

Principles for Internet Use -  
Children's Version Be SMART On Line

S	<b>Secret</b> - Never give your address, telephone number, username or password when online
M	<b>Meeting</b> someone or a group you have contacted on-line is not allowed without the permission and supervision of your parent or teacher.
A	<b>Accepting</b> e-mails, opening sites or files requires the permission of your teacher, appointed adult or parent.
R	<b>Remember</b> no offensive language, text or pictures are to be displayed, sent, copied or received.
T	<b>Tell</b> your parent, teacher or trusted adult if someone or something makes you uncomfortable.

# Think then Click



These rules help us to stay safe on the Internet

We only use the internet when an adult is with us



We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.



We always ask if we get lost on the Internet.

We can send and open emails together.



We can write polite and friendly emails to people that we know.



# Think then Click

## e-Safety Rules for Key Stage 2



We ask permission before using the Internet.



We only use websites that an adult has chosen.



We tell an adult if we see anything we are uncomfortable with.



We immediately close any webpage we are not sure about.



We only e-mail people an adult has approved.



We send e-mails that are polite and friendly.



We never give out personal information or passwords.



We never arrange to meet anyone we don't know.



We do not open e-mails sent by anyone we don't know.



We do not use Internet chat rooms.

*Points for Children to Consider*

**Follow These SMART TIPS**



**Secret** - Always keep your name, address, mobile phone number and password private - it's like giving out the keys to your home!



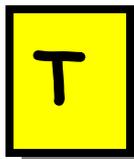
**Meeting** someone you have contacted in cyberspace can be dangerous. Only do so with your parent's/carer's permission, and then when they can be present.



**Accepting** e-mails or opening files from people you don't really know or trust can get you into trouble - they may contain viruses or nasty messages.



**Remember** someone on-line may be lying and not be who they say they are. Stick to the public areas in chat rooms and if you feel uncomfortable simply get out of there!



**Tell** your parent or carer if someone or something makes you feel uncomfortable or worried.

SMART Tips from: - Helping your parents be cool about the Internet, produced by:  
Northern Area Child Protection Committees

Before you text, type  
or speak, **THINK** first

**T** - is it **TRUE**?

**H** - is it **HELPFUL**?

**I** - is it **INSPIRING**?

**N** - is it **NECESSARY**?

**K** - is it **KIND**?

## **ICT Code of Safe Practice for Staff**

### **eSafety Rules**

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school.

This code of practice is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT.

All staff are expected to agree to this code of practice and adhere at all times to its contents.

Any concerns or clarification should be discussed with Mr Torney (Principal & school E-Safety coordinator)

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Principal or Board of Governors.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, C2k, secure e-mail system for any school business.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- Personal data can only be taken out of school or accessed remotely when authorised by the Principal or Board of Governors. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of Mr Magee
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Principal.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Principal.

- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

### **User Signature**

I agree to follow this code of practice and to support the safe and secure use of ICT throughout the school

Signature \_\_\_\_\_ Date \_\_\_\_\_

Full Name \_\_\_\_\_ (printed)

**Using Children's Photographs in St Patrick's PS**

**I agree to my child's photograph appearing in the local press,  
on the school website and on school displays.**

**I understand that no contact details will be published.**

Child's Name: \_\_\_\_\_ Class: \_\_\_\_\_

Parent/Guardian's Name: \_\_\_\_\_

Parent/Guardian's Signature: \_\_\_\_\_

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

OR

**I do not agree to my child's photograph appearing in the press  
or on a school website.**

Child's Name: \_\_\_\_\_ Class: \_\_\_\_\_

Parent/Guardian's Name: \_\_\_\_\_

Parent/Guardian's Signature: \_\_\_\_\_

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