# E SAFETY POLICY
# FOR
# SAINT COLUMBAN'S P.S.
# BELCOO

Signed:

*Gerry McAloon* *12-04-2022*

Chair of Board of Governors Date

*Liam Magee* *12-04-2022*

Principal Date

*Anne Murray* *12-04-2022*

ICT Co-ordinator Date

# *E-SAFETY POLICY*

## INTRODUCTION:

Boards of Governors have a duty to safeguard and promote the welfare of pupils (Article 17 of the Education and Libraries (Northern Ireland)
Order 2003). It is also the duty of the Board of Governors to determine the measures to be taken at a school to protect pupils from abuse (Article 18 of the Education and Libraries (Northern Ireland) Order 2003 refers).
In the exercise of those duties, Boards of Governors must ensure that their schools have a policy on the safe, healthy, acceptable and effective use of the Internet and other digital technology tools. They must also actively promote safe and acceptable working practices for all staff and pupils: these will serve to reassure parents and guardians.

This E-safety policy contains policies in relation to use of the internet, use of mobile phones and use of digital/photographic images of children. It is largely based on DENI Circular 2007/1 *"Acceptable Use of the Internet and Digital Technologies in Schools"*, DENI Circular 2011/22 *"Internet Safety"* and DENI Circular 2013/25 *"eSafety Guidance". 2016/*26 Effective Uses of Mobile Digital Devices, 2016/27 Online Safety.
It should also be read in conjunction with the School's Child Protection Policy.

## INFORMATION AND COMMUNICATIONS TECHNOLOGY:

Introduction Information and Communications Technology (ICT) covers a wide range of resources including web-based and mobile learning.
Currently the internet technologies children and young people are using, both inside and outside of the classroom, include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis • Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/Smart phones with text, video and/or web functionality
- Other mobile devices with web functionality

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 Columban's PS we understand the responsibility to educate our pupils in eSafety issues. We aim to teach them 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.

**What is e-Safety?**

- E-Safety is short for 'electronic safety'.
- It highlights the responsibility of the school, staff, governors and parents to mitigate risk through reasonable planning and actions. E-Safety covers not only Internet technologies but also electronic communications via mobile phones, games consoles and wireless technology.

E-Safety in the school context:

- is concerned with safeguarding children and young people in the digital world;
- emphasises learning to understand and use new technologies in a positive way;
- is less about restriction and focuses on education about the risks as well as the benefits so that users feel confident online;
- is concerned with supporting pupils to develop safer online behaviours both in and out of school; and
- is concerned with helping pupils recognise unsafe situations and how to respond to risks appropriately. **(ref: DE Circular 2013/25)**

## THE INTERNET

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. 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.

The DENI circular 2007/01 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 the safe and effective use of the Internet in St Columban's Primary School.
The policy has been drawn up by the staff of the school under the leadership of the Principal and ICT Co-ordinator.
It has been approved by the Board of Governors and is available to all parents via the school website and as a hard copy, if requested.

## C2K

Classroom 2000 (C2k) is the project responsible for the provision of an information and communications technology (ICT) managed service to all schools in Northern Ireland. It provides a safety service which should ensure educational use made of resources is safe and secure, while protecting users and systems from abuse.
Some of these safety services include:

- Providing all users with a unique user names and passwords
- Tracking and recording all online activity using the unique user names and passwords
- Scanning all C2k email and attachments for inappropriate content and viruses
- Filters access to web sites
- Providing appropriate curriculum software.

Should the school decide to access online services through service providers other than C2k then we will ensure that effective firewalls, filtering and software monitoring mechanisms are in place.

### POTENTIAL CONTACT

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

### EDUCATION OF PUPILS:

- People are not always who they say they are.
- "Stranger Danger" applies to the people they encounter through the Internet.
- They should never give out personal details.
- They should never meet alone anyone contacted via the Internet, and
- Once they publish information it can be disseminated with ease and cannot be destroyed.

### USEFUL RESOURCES:

Child Exploitation and Online Protection (CEOP) – www.thinkuknow.co.uk Childnet International – www.childnet.com

Project Evolve Toolkit – www.projectevolve.co.uk

### 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, e.g. some use the web to publish 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 should 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.

## EXCESSIVE COMMERCIALISM

The Internet is a powerful vehicle for advertising. In visiting websites children have easy access to advertising which is very persuasive.

Children should be taught:

- not to fill out forms with a lot of personal details.
- not to use an adult's credit card number to order online products.

If children are to use the Internet in places other than at school e.g. – libraries, clubs and at home, they need to be educated about how to behave on-line and to discuss problems. There are no totally effective solutions to problems of Internet safety. Teachers, pupils and parents must be vigilant.

## Roles and Responsibilities

- As e-Safety is an important aspect of strategic leadership 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 update Governors with regard to e-safety so that all governors have an understanding of the issues at our school in relation to local and national guidelines and advice.

## Writing and Reviewing the e-Safety Policy

- This policy, supported by the school's Acceptable Use Agreement for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community.
- It is linked to other school policies including those for ICT, Positive Behaviour, Health and Safety, Child Protection, and Anti-bullying.
- It has been agreed by the Senior Leadership Team, Staff and approved by the Governing Body.

- The e-Safety policy and its implementation will be reviewed biennially.

**E-Safety Skills' Development for Staff**

- All staff receive regular information and training on e-Safety issues through the coordinator 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 receive information on the school's Acceptable Use Agreement as part of their induction.

- All staff are encouraged to incorporate e-Safety activities and awareness within their lessons.

- E-safety training is part of an on-going CPD programme.

- Additional support and advice is available from C2k, Social services or the PSNI if required.

**Child Protection / Safeguarding Designated Teacher:**
Are trained in e-safety issues and aware of the potential for serious child protection and safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

**E-Safety Information for Parents/Carers**

- Parents/carers are asked to read through and sign the Acceptable Use Agreement on behalf of their child.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used on the school website.

- The school website contains useful information and links to sites like CEOP's thinkuknow, Childline, and the CBBC Web Stay Safe page.

- The school will communicate relevant e-Safety information through newsletters, the school website and e-Safety talks.

- Parents should remember that it is important to promote e-Safety in the home and to monitor Internet use.

- Keep the computer in a communal area of the home.

- Be aware that children have access to the internet via gaming stations and portable technologies such as smart phones.

- Monitor on-line time and be aware of excessive hours spent on the Internet. • Take an interest in what children are doing. Discuss with the children what they are seeing and using on the Internet.

- Advise children to take care and to use the Internet in a sensible and responsible manner. Know the SMART tips.
- Discuss the fact that there are websites/social networking activities which are unsuitable.
- Discuss how children should respond to unsuitable materials or requests.
- Remind children never to give out personal information online.
- Remind children that people on line may not be who they say they are.
- Be vigilant. Ensure that children do not arrange to meet someone they meet on line.
- Be aware that children may be using the Internet in places other than in their own home or at school and that this internet use may not be filtered or supervised.

**Teaching and Learning 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 is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are aware of the impact of online bullying and know how to seek help if these issues affect them. Pupils are also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/carer, teacher/trusted member of staff, or an organisation such as Childline/CEOP.
- 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.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Children are taught to be 'Internet Wise'. Children are made aware of Internet Safety Rules and are 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 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 are not always 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 are supervised by the teacher.

Social Networking:

- The school C2k system will block access to social networking sites for pupils. • 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; Pupils will be advised never to give out personal details of any kind which may identify them or their location.
  - Pupils should be advised not to place personal photos on any social network space.
  - Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.
- Our pupils are asked to report any incidents of bullying to the school.

- School staff will not add children as 'friends' if they use these sites.

**School Web Site**

The school web site is used to celebrate pupils' work, promote the school and provide information. Editorial guidance will ensure that the Web site reflects the school's ethos that information is accurate and well presented and that personal security is not compromised. An editorial team ensure common values and quality control. As the school's Web site can be accessed by anyone on the Internet, the school has to be very careful to safeguard the interests of its pupils and staff. The following rules apply.

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site (see Appendix 3).
- Pupils' full names will not be used on the Web site, particularly in association with photographs.

- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

**Mobile Technologies:**

• The use of portable media such as memory sticks and external hard drives will be monitored closely as potential sources of computer virus and inappropriate material.

• Staff should not store pupils' personal data and photographs on memory sticks. • Pupils are not allowed personal mobile devices/phones in school.

• Staff should not use personal mobile phones during designated teaching sessions.

**Managing Video-conferencing**:

• Videoconferencing will be via the C2k network to ensure quality of service and security.

• Videoconferencing will be appropriately supervised.

**Publishing Pupils' Images and Work:**

• Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website / twitter account. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue.

• Parents/carers may withdraw permission, in writing, at any time.

• Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.

• Pupils' full names will not be used anywhere on the School Website, particularly in association with photographs.

• Pupils' work can only be published by outside agencies with the permission of the pupil and parents.

**Policy Decisions: Authorising Internet access**

• Improved Websense filtering gives the school flexibility to control and develop the Internet Filtering. The ICT Co-ordinator is responsible for filtering access.

• Pupil instruction in responsible and safe use should precede any Internet access and all children must sign up to the Acceptable Use Agreement for pupils and abide by the school's e-Safety rules. These e-Safety rules will also be displayed clearly in all rooms.

• Access to the Internet will be supervised.

- All parents will be asked to sign the Acceptable Use Agreement for pupils giving consent for their child to use the Internet in school by following the school's e-Safety rules and within the constraints detailed in the school's e-Safety policy.

- All staff must read and agree in writing to adhere to the Acceptable Use Agreement for Staff before using any school ICT resource.

**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 are aware of their individual responsibilities to protect the security and confidentiality of the school network, MIS systems.

**Handling e-Safety Complaints:**

- Complaints of Internet misuse will be dealt with by a senior member of staff (Principal, ICT Co-ordinator + Pastoral Care Co-ordinator).

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Co-ordinator.

- Any complaint about staff misuse must be referred to the Principal.

- Complaints of a Child Protection nature must be dealt with in accordance with school Child Protection procedures.

**Communicating the Policy:**

Introducing the e-Safety Policy to pupils

- e-Safety rules will be displayed in all classrooms and discussed with the pupils at the start of each year. Specific lessons will be taught by class teachers at the beginning of every year and at relevant points throughout e.g. during PDMU lessons/circle times/anti-bullying week.

- Pupils will be informed that network and Internet use will be monitored. .

**Parents and the e-Safety Policy:**

- Parents will be asked to sign an agreement giving their child permission to use the internet within school.

- Parents will be given an outline of the Policy and informed that the full policy is available on the school website.

- Parents will be informed that network and Internet use will be monitored.

## Staff and the e-Safety Policy:

- All staff will be given the School e-Safety Policy and its importance explained.
- Any information downloaded must be respectful of copyright, property rights and privacy.
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential.
- A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software, both in and out of school. (ref: DE Circular 2013/25)

## Code of Practice for Staff

The following Code of Safe Practice has been agreed with staff: (ICT Safe Code of Practice Agreement which staff are asked to sign when taking up post is attached for information Appendix 1)

## Code of Safe Practice for Pupils

A parental/carer consent letter (Appendix 2) accompanied by the code of practice for pupils is sent out annually to parents/carers and this consent along with that of the pupil (post primary) must be obtained before the pupil accesses the internet.

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

- The school's eSafety code of practice for Use of the Internet and other digital technologies is made explicit to all pupils and eSsafety guidelines are displayed prominently throughout the school;
- Our Code of Practice is reviewed each school year and signed by pupils/parents;
- 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, where possible;
- 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 websites.

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 pupils are forbidden to access social networking sites.

## Monitoring and review:

This policy is implemented on a day-to-day basis by all school staff and is monitored by the ICT Co-ordinator.

This policy is the Governors' responsibility and they will review its effectiveness every 2 years. They will do this during reviews conducted between the ICT Co-ordinator and Designated Child Protection Co-ordinator.

## Appendix 1

### 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 Mrs Murray school eSafety coordinator or Mr Magee (Principal)

- 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 of 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, with a school camera / Ipad 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)   Job Title . . . . . . . . . . . . . . . .

**Appendix 2**

# Parental Agreement/Consent Letter

Dear Parent

As part of St Columban's PS Information and Communications Technology programme we offer pupils supervised access to a *filtered* Internet service provided by C2k. Access to the Internet will enable pupils to explore and make appropriate use of many web sites that are of enormous educational benefit.
They can also exchange messages with other Internet users throughout the world. However in spite of the tremendous learning potential, you should be advised that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people.

In order to help minimise any risks, which might arise from Internet use, our Service provider C2k has installed filtering software which operates by blocking thousands of inappropriate web sites and by barring inappropriate items, terms and searches in both the Internet and e-mail. To further enhance safety, pupils will only use the Internet for educational purposes, under the supervision of a member of staff.

The school's rules for safe Internet use accompany this letter. Please read and discuss these with your child and return the attached page.

If you have any concerns or would like some explanation please contact myself.

Yours sincerely

Mr Liam Magee
Principal

## ICT Code of Safe Practice

### Pupil - An Acceptable Use of the Internet

Children should know that they are responsible for following our Acceptable Use of the Internet rules.

They must discuss and agree rules for this Acceptable Use.

Parents are also asked to be aware of the code of Acceptable Use and confirm that their children will follow these rules.

- 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 only open/delete my own files.
- I will not bring in memory sticks or CD Roms from home to use in school unless I have been given permission by my class teacher.
- I will use the Internet for research and school purposes only.
- I will only use my class e-mail address or my own school e-mail address when e-mailing.
- I will only open e-mail attachments from people I know, or who my teacher has approved.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my eSafety.
- If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately
- I will follow all school rules / guidelines in relation to online remote learning

# Acceptable Use of the Internet

# Parental Consent Form

We have discussed the E Safety rules and ………………………….

(child name) agrees to follow these rules and to support the safe use of ICT at St Columban's Primary School.

I understand that students will be held accountable for their own actions concerning their use of all ICT equipment.

I understand that some of the materials on the Internet may be objectionable and I support the School in setting standards for my child/ren to follow when selecting, sharing and exploring information and computer based media.

Parent/Guardian's Name: __________________________

Parent/Guardian's Signature: __________________________

Date: __________________________

**Appendix 3**

# Using Children's Photographs in St Columban's PS

**I understand that my child's photograph or video image may be used for school and curriculum purposes during their time at St Columban's PS and beyond this for historical reasons. These may be used for displays, newsletters, school website school twitter and press releases to promote a positive image of the school.**
**I understand that no contact details will be published.**

I agree to the above conditions regarding the use of my child's photographs / videos.

Child's Name: ______________________________

Parent/Guardian's Name: ______________________________

Parent/Guardian's Signature: ___________________________

Date: ___________________________

---------------------------------------------------------------------

**I do not agree with the above conditions and do not wish my child's photograph or video to be used.**

Child's Name: ______________________________

Parent/Guardian's Name: ______________________________

Parent/Guardian's Signature: ___________________________

Date: ___________________________

**If you wish to change your mind regarding the choice you have made please contact the Principal for a new form.**

## Sample Posters

### Key Stage 1

# 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.

B. Stoneham & J. Barrett

Key Stage 2

# 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 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.

## Principles for Internet Use ----- Children's Version

Be **SMART** On Line

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

# Smile and Stay Safe Poster

**eSafety guidelines to be displayed throughout the school**

## SMILE and stay safe

**S**taying safe means keeping your personal details private, such as full name, phone number, home address, photos or school.

**M**eeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

**I**nformation online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'

**L**et a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

**E**mails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

## Additional Advice for Parents with Internet Access at home

1. A home computer with Internet access should be situated in a location where parents can monitor access to the Internet.

2. Parents should agree with their children suitable days/times for accessing the Internet.

3. Parents should discuss with their children the school rules for using the Internet and implement these at home. Parents and children should decide together when, how long and what constitutes appropriate use;

4. Parents should get to know the sites their children visit and talk to them about what they are learning;

5. Parents should consider using appropriate Internet filtering software for blocking access to unsavoury materials. Further information is available from Parents' Information Network (address below);

6. It is not recommended that any child under 16 should be given unmonitored access to newsgroups or chat facilities;

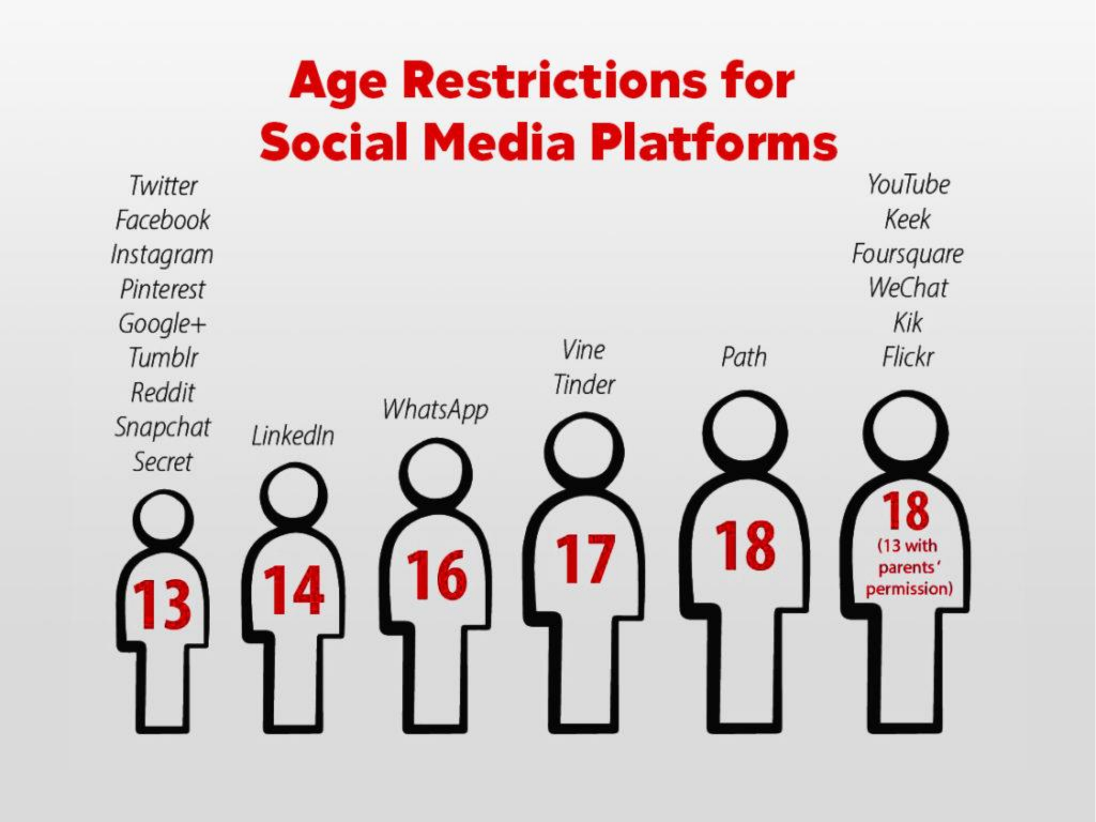
7. Parents should ensure that they give their agreement before their children give out personal identifying information in any electronic communication on the Internet, such as a picture, an address, a phone number, the school name or financial information such as credit card or bank details. In this way they can protect their children and themselves from unwanted or unacceptable overtures from strangers, from unplanned expenditure and from fraud.

8. Parents should 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.

Further advice for parents is available from the following sources:

- http://www.thinkuknow.co.uk Thinkuknow - a mock cybercafé which uses online role-play to help children from 5 to 16+ explore a range of issues.
- http://www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf Aimed at parents and carers, there is a great deal of very clear information about chat rooms, social networking sites, email and much more.
- http://www.parentscentre.gov.uk/usingcomputersandtheinternet A very comprehensive site aimed at parents and carers. Includes many articles and external links to other helpful sites.
- http://www.bbc.co.uk/webwise Includes an 'Internet for Beginners' course and a tool for answering your internet related questions.
- http://www.kidsmart.org.uk/ Explains the SMART rules for safe internet use and lots more besides.
- http://www.ceop.gov.uk/ The government's Child Exploitation and Online Protection Centre (CEOP)
- http://www.parents.vodafone.com Vodafone's site is designed to help parents and carers develop an understanding of their child's internet use.

For useful help with setting safety and privacy settings on social media apps visit: https://parentzone.org.uk/article/setting-safety-and-privacy-settings-social-media-apps


Age Restrictions for Social Media Platforms

13+
TikTok
16+
18