St. Colmcille's Primary School

E-Safety Policy

Date Approved by the Board of Governors: 5th March 2019

Signed: Diarmuid O'Loan
Chairperson of the Board of Governors

Next Policy Review Date: (+3 years)

Guidelines for using the Internet and Digital Technologies in St. Colmcille's Primary School

1. Introduction

The Board of Governors will ensure that St. Colmcille's Primary school has a policy on the safe, healthy, acceptable and effective use of the Internet and other digital tools e.g. digital cameras and acceptable use of mobile phones which have downloadable capabilities. They also promote safe and acceptable practices for all staff and pupils.

2. General

Use of ICT in the Northern Ireland education community must be in support of the aims and objectives of the Northern Ireland Curriculum

- All users must comply with all copyright laws;
- All users must limit their use of the Internet for school related purposes – examples of this include the use of email, the use of the Internet to investigate and research school subjects and staff using the Internet to further develop their professional development;
- All users are expected to behave in an appropriate manner when communicating with others;
- All users must be aware that the use of the Internet in schools is a privilege and not a right and this privilege will be withdrawn if it is misused;
- All users must respect the hardware and software that has been made available to them;
- All users must respect the work of others.

3. **Code of Conduct for Staff** (See Appendix 1)

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

- Staff will participate in annual E-Safety updates.
- 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.
- Staff will not bring in software, USB Hardware into school without permission.
- 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.
- Access to SIMS should only be made with each staff member's username and password.

4. **Code of Conduct for Pupils** (See Appendix 2)

Pupils will be taught that the responsible and safe use of the internet 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 Think Then Click (KS1) (Appendix **7**), Acceptable Use Rules & SMART Tips (KS2) (Appendix 8). These e-Safety rules will also be displayed clearly in all rooms.

- I will access the system with my login and password.
- I will not access other people's files without permission.
- I will only use the computers, Internet, My School for school work and homework.
- I will not bring in software, USB Hardware into school without permission.
- I will ask permission from a member of staff before using the Internet.
- I will only e-mail people I know, or my teacher has approved.
- I will not open e-mails sent by someone I don't know and report any unpleasant material or messages sent to me.
- The messages I send will be polite and responsible.
- I will not give my name, home address, telephone number, or arrange to meet someone.
- I will not bring a mobile phone into school without written parental permission.
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will never give out personal information.

4. **PUPIL SANCTIONS**

Pupils must follow the St. Colmcille's Primary School Internet Use Agreement. Any violation of the regulations (See Appendix 2) is unethical and may constitute a criminal offence. Should any violation be committed;

1. Access privileges may be revoked; and
2. School disciplinary action in line with the school discipline policy and/or appropriate legal action may be taken.

Use of the school's Internet account is a privilege, not a right.

The Internet is to be used for educational and research purposes only, consistent with the educational aims of the School. Misuse will result in loss of the account.

Staff may monitor pupil use of the Internet, including e-mail, to determine that use is for the stated purposes. For this and other reasons, e-mail is not private. Violations that may lead to cancellation of Internet access include:

- Playing computer based games;
- Downloading excessively large files;
- E-mail correspondence inappropriate to educational purposes;
- Any activity posing potential risks to themselves or others;
- Harassing other users (e.g. with unwanted e-mail messages);
- Illegal activity;
- Revealing any person's home address/phone number;
- Vandalism of accounts or systems;
- Using abusive, vulgar, or other inappropriate language;
- Viewing or downloading inappropriate images;
- Failure to report known security problems; and
- Any other inappropriate use or misuse of the facility.

Staff at St. Colmcille's Primary School will deem what is inappropriate use, and their decision is final. Accounts are monitored and use of the account implies agreement to such monitoring. Staff may close an account at any time for violations.

5. **<u>Information for Parents</u>** (See Appendix 3 and 5)

- **Parents are aware of the images they take and where and when they use them. Posting images onto any Social Websites or using material without the permission of other parents is illegal and taken seriously by the PSNI.**

- Parents should be aware that the access to the Internet provided to staff and pupils in school has limiting security features.

- Parents should be aware that the use of the Internet in school is closely monitored by staff.

- Parents should be aware that there will be no use of the Internet without the supervision of staff and that this will be in full view of others, e.g. the classroom or ICT Suite.

- Parents should, in co-operation with staff, make pupils aware of the rules and expectations within the Code of Conduct Agreement.

- Parents should be aware that the use of ICT is used as a tool to complement and enhance prior learning– i.e. the use of computers, iPads etc.

- Parents should be aware that children's full names will not be available online at any stage but their work may be displayed on the School Website and social media platforms where permission has been given.

- Parents should be aware that no photographs of pupils will be available online without parents giving their permission. Group and individual photographs will be used excluding the pupils' full names.

- Parents should be aware that mobile phones are not permitted in school, without written consent, on the grounds that Internet access becomes very difficult to monitor.

- Parents should also be aware that social networking sites such as Snapchat, Facebook and Twitter adhere to a strict 'over 13s' age policy.
- Parents should be aware that the School Website contains useful information and links to sites like thinkuknow, Childline, Safer Internet Day website, BBC Learning Zone, EA.
- Parents should be aware that the school will communicate relevant e-Safety information through newsletters and the school website.

6. **Parental Responsibility** (Appendix 3)

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

7. **Teaching and Learning**

(a) 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.
- E-Safety will be at an age appropriate level and with a two week focus in February.
- 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.
- 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.

(b) 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.
- 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.
- 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.
- Parents will be advised not to post photos/videos on Social Networking sites.

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.
- Unless written permission has been given by parents, pupils are not allowed to have personal mobile phones in school.

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 or Social Media.
- Parents/carers may withdraw permission, in writing, at any time.
- Pupils' full names will not be used anywhere on the School Website in association with photographs.
- Pupil's work can only be published by outside agencies with the permission of the pupil and parents.
- **Parents are aware of the images they take and where and when they use them. Posting images onto any Social Websites or using material without the permission of other parents is illegal and taken seriously by the PSNI.**

Policy Decisions:

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.

Handling e-Safety Complaints:

- Complaints of Internet misuse will be dealt with by the Leader of ICT.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Leader of ICT and recorded in the e-Safety incident logbook. (**Appendices 4 and 6**)
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with the school's safeguarding and child protection procedures. (See Safeguarding and Child Protection Policy)
- Pupils and parents will be informed of the complaint's procedure.

Training for parents

E-Safety workshops for parents.

Addendum

Network administrators reserve the right to review files and communications to maintain system integrity and ensure that the users are using the system responsibly – they will respect the right to privacy whenever possible

This document is based on

Acceptable Use of the Internet and Digital Technologies in Schools
(DENI Circular 2007/1 – 18 June 2007)
http://www.deni.gov.uk/22-acceptable_use_of_the_internet_de_circular.pdf

Appendix 1

St. Colmcille's Primary School

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 Leader of ICT.

- 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.
- Access to SIMS should only be made with each staff member's username and password.

Name		
Date		**Signed**

Appendix 2

ICT Code of Practice Agreement for Pupils

Years 3-7

Parents - please read this agreement with your child before signing.

St. Colmcille's Primary School have computers, iPads and Internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will access the system with my login and password.
- I will not access other people's files without permission.
- I will only use the computers, Internet, My School for school work and homework.
- I will not bring in software, USB Hardware into school without permission.
- I will ask permission from a member of staff before using the Internet.
- I will only e-mail people I know, or my teacher has approved.
- I will not open e-mails sent by someone I don't know and report any unpleasant material or messages sent to me.
- The messages I send will be polite and responsible.
- I will not give my name, home address, telephone number, or arrange to meet someone.
- I will not bring mobile phones into school (unless I have written parental consent).
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will never give out personal information or passwords.

Signed by child: _____

Signed by parent/guardian: _____

Date: _____

Appendix 3

Parent Agreement

As the parent or guardian of this pupil, I have read the Code of Practice Agreement. I understand that this access is designed for educational purposes. I recognise that it is impossible to restrict access to all controversial materials, and I will not hold St. Colmcille's Primary School responsible for any improper or illegal use of the Internet in school by my child. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to permit Internet access for my child and certify that the information contained on this form is correct.

Signed: _____ (Parent) Dated: _____

Parent Consent Forms

(to be completed by all parents)

Child's Name: _____

I am aware that if I take images or videos during a school event that posting these onto any Social Websites or using material without the permission of other parents is illegal and taken seriously by the PSNI.

Signed: _____ (Parent) Dated: _____

I give / do not* give permission for photographs of my child, my child's name and/or my child's work to be displayed around the school or in community displays.

Signed: _____ (Parent) Dated: _____

* delete as appropriate

I give / do not* give permission for photographs of my child, my child's first name and / or my child's work to be used in the local press or displayed on the school website.

Signed: _____ (Parent) Dated: _____

* delete as appropriate

Appendix 4

E-Safety Incident Log

Name: _____ Class: _____ Date: _____

Teacher in charge: _____

Details of incident & Action Taken

Appendix 5

E-Safety Information for Parents/Carers

E-safety tips for Parents of Primary School Children

79% of 7-11 year-olds said they would tell their parent or carer if something worried them online.

Childnet, Have your Say (2013)

Checklist

Put yourself in control
Make use of the parental controls on your home broadband and any internet-enabled devices. You can find out how at your broadband provider's website or by visiting internetmatters.org.

Search safely
Use safe search engines such as swiggle.org.uk or kids-search.com. Safe search settings can also be activated on Google and other search engines as well as YouTube. You can find out more at google.co.uk/safetycentre.

Agree boundries
Be clear what your child can and can't do online – where they can use the internet, how much time they can spend online, the sites they can visit and the type of information they can share. Agree with your child when they can have a mobile phone or tablet.

Explore together
The best way to find out what your child is doing online is to ask them to tell you about it. Put the family computer in a communal area so you can see what sites they're visiting and share with them.

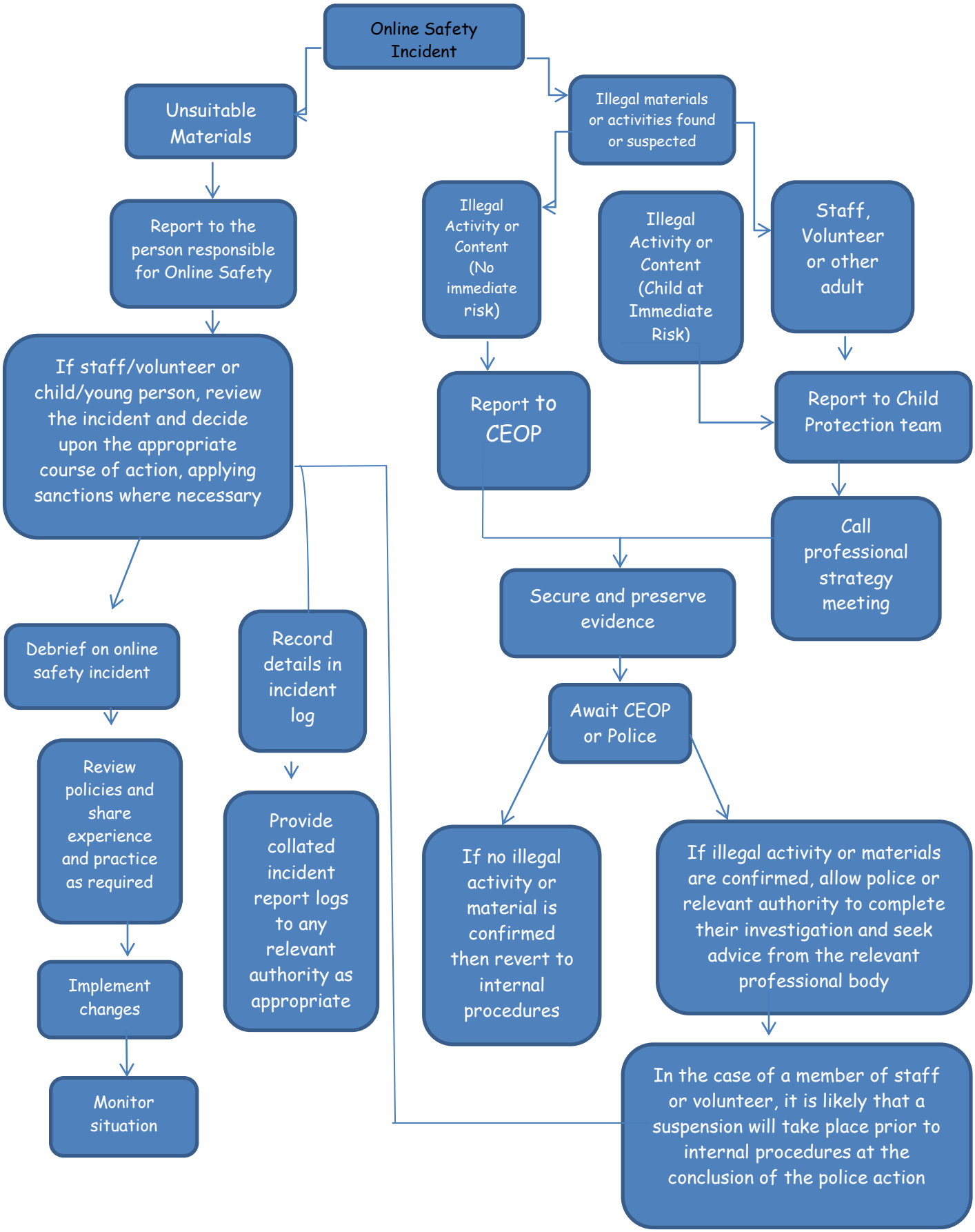
Check if it's suitable
The age ratings that come with games, apps, films and social networks are a good guide to whether they're suitable for your child. The minimum age limit is 13 for several social networking sites, including Facebook and Instagram.

Know this stuff matters,
but don't know where to turn?

Internet Matters is a free online resource for every parent in the UK. We'll show you the best ways to protect your children online – with information, advice and support on all the big e-safety issues.

internet matters.org

Appendix 6 **Flow chart of procedures to follow an E-Safety incident**



Appendix 7

These rules help us to stay
safe on the Internet

Think then Click

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.

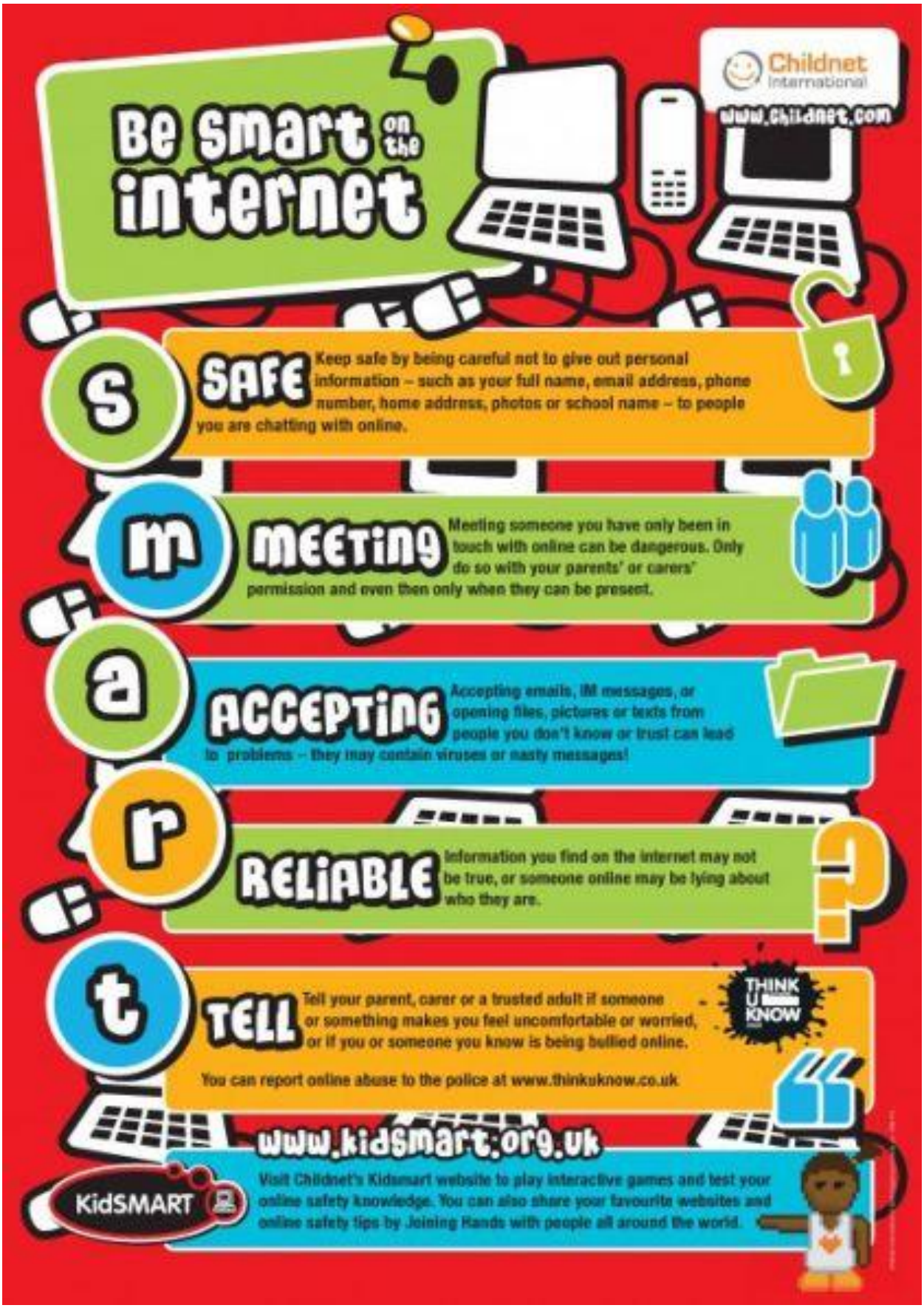
We can search the Internet with an adult.

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.

Appendix 8


Childnet International
www.childnet.com
Be smart on the internet
S
SAFE
Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.
m
MEETING
Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.
a
ACCEPTING
Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!
r
RELIABLE
Information you find on the internet may not be true, or someone online may be lying about who they are.
t
TELL
Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
THINK U KNOW
You can report online abuse to the police at www.thinkuknow.co.uk
www.kidsmart.org.uk
KidSMART
Visit Childnet's Kidsmart website to play interactive games and test your online safety knowledge. You can also share your favourite websites and online safety tips by Joining Hands with people all around the world.