Summerville Primary School Policy for Acceptable Use of ICT and E-Safety

Date	February 2016
Review Date	February 2017
Chair of Governors	Michelle Duval
Signature	
Head Teacher	Joanne Jordan
Signature	

Introduction

Our policy applies to all students, staff, governors and volunteers associated with Summerville Primary School. The 'staying safe' outcome of Every Child Matters is at the heart of the policy.

The 'staying safe' outcome includes aims that children and young people are:
- safe from maltreatment, neglect, violence and sexual exploitation
- safe from accidental injury and death
- safe from bullying and discrimination
- safe from crime and anti-social behaviour in and out of school
- secure, stable and cared for.

These aims apply just as much to the 'virtual world' as the physical world. Children and young people may encounter dangers whenever they use ICT in its various forms. It is the duty of the school and its staff to ensure that every child in our care is safe when using technology, as in other contexts.

It is, however, equally important to recognise that technology and more specifically the internet is possibly the single most powerful learning resource available today, and when properly used can broaden the horizons of children and help prepare them for the wider world.

There are 6 areas of this policy:

1. Acceptable Use of ICT
2. Current Technologies
3. Social networking
4. E-Safety Risks
5. Strategies to Minimise the Risks
6. How will complaints regarding e-Safety be handled?

7. Staff Code of Conduct for ICT (Appendix 1)
8. Home School E-Safety Agreement (Appendix 2)

1. Acceptable use of ICT

All staff and pupils within the school are expected to behave in a responsible manner when using ICT equipment. All staff are responsible for ensuring that children using ICT equipment use it in ways which are appropriate, and which minimise the risk of exposure inappropriate material.

Staff may not use the school's ICT equipment for personal use and must ensure that all sensitive data is stored in a manner which is in keeping with the Data Protection Act 1998 and all other legislation.

2. Current Technologies

ICT provides many essential tools for modern education and the internet is an invaluable resource for learning. For this reason we must simultaneously embrace new technologies whilst being vigilant against the risks presented by these technologies to the children in our care.

New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet
    - o Browsing
    - o Email
    - o Instant messaging often using simple web cams
    - o Blogs (an on-line interactive diary)
    - o Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
    - o Social networking sites
    - o Video broadcasting sites
    - o Chat Rooms
    - o Gaming Sites
    - o Music download sites
- Mobile phones with internet, camera and video functionality
- Mobile technology (e.g. games consoles) that are 'internet ready'.

3. Social Networking

It is important to ensure you maintain a high level of professionalism and behaviour when using social networking sites. The following guidelines should be followed:

- Make sure that do not have any pupils as friends including past pupils.

- Make sure that your privacy settings prevent anybody other than your friends gaining access to your profile.
- Where possible you should not be friends with parents. If you are friends with an ex-employee of the school or if you are a parent and a member of staff you must remove any content relating to other members of staff and make no comments that can be connected to your role at school. Any comments or actions that can be considered to bring the school into disrepute will be taken very seriously.

4. E-Safety Risks

The risks can be summarised under the following headings as identified in Becta's Safeguarding Children in a Digital World (2006) advice:

a) Exposure to age-inappropriate material
b) Exposure to inaccurate or misleading information
c) Exposure to socially unacceptable material, such as that inciting violence, hate or intolerance
d) Exposure to illegal material, such as images of child abuse
e) Grooming using communication technologies, leading to sexual assault and/or child prostitution
f) Exposure of minors to inappropriate commercial advertising
g) Exposure to online gambling services
h) Commercial and financial scams
i) Bullying via websites, mobile phones or other forms of communication device
j) Downloading of copyrighted materials e.g. music and films

5. Strategies to Minimise the E-Safety Risk

a) E-safety education as a part of the curriculum
b) *RM Safetynet* internet filtering screens all internet traffic coming into the school
c) A signed E-safety Agreement between the school, pupils and parents
d) All parents / carers consent for web publication of work and photographs
e) Age appropriate e-Safety rules displayed in all classrooms (Appendix 3)
f) E-bullying to be addressed during anti bullying week's assembly
g) Child protection issues to be reported direct to the named persons: Joanne Jordan (Headteacher), Mandy Gilluley (Learning Mentor) or David Nightingale (Deputy Headteacher)
h) E-Safety concerns reported direct to Joanne Jordan (Headteacher)
i) The use of all new technologies is to be monitored by all staff
j) All staff sign a Code of Conduct for ICT.   (Appendix 1)

4. How will complaints regarding E-Safety be handled?

The school will take all reasonable precautions to ensure E-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is impossible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Any complaint about staff misuse is referred to Joanne Jordan (Headteacher).

Appendix 1
Staff Code of Conduct for ICT
Appendix 2
Home School E-Safety Agreement
Appendix 3
School e-safety Rules

Summerville Primary School
Policy for Acceptable Use of ICT and E-Safety

<u>**Appendix 1 - Staff Code of Conduct for ICT**</u>

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras; email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator (David Nightingale), the Designated Child Protection officer (Mandy Gilluley) or the Headteacher (Joanne Jordan).
- I will ensure that electronic communications with pupils including email, instant mail and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will not disable any safe search settings on any search engine, and I will enable any such settings where possible before allowing children to use a search engine.
- During school hours all staff must keep mobile telephones turned off, except when such devices are being used as a means of emergency contact on school trips, or by express permission of the Headteacher.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I give permission for images of me to be used on the school website and on other materials produced by the school.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: ……………………………… Capitals: ……………………… Date: ………………

Accepted for school: ……………………………. Capitals: …………………………….

Summerville Primary School
Policy for Acceptable Use of ICT and E-Safety

Appendix 2 - Home School E-Safety Agreement

Home School E-Safety Agreement
It is an essential part of learning, and National Curriculum requirement, for all pupils to use computer facilities including Internet access. Pupils and their parents or carers are required to sign agreeing to our e-Safety Rules.

Pupil:	*Class:*

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	*Date:*

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	*Date:*

Please print name:

Please complete, sign and return to the school secretary

Appendix 3.1 - School e-safety Rules (Years 4-6)

Years 4-6

Think then Click
These rules help us to stay safe on the internet in school and at home.
- We tell an adult if someone we don't know asks for personal information on the internet.   - We tell an adult if we receive an email which is not nice.   - We ask permission before using the Internet.   - We only use websites that an adult has said are ok.   - 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.   - We do not download anything without checking that it is ok first. (e.g. music or software)

Appendix 3.2 - School e-safety Rules (Years 1-3)

Years 1-3

Think then Click

These rules help us to stay safe on the internet
in school and at home.

We only use the internet when an adult is with us.

We always ask if we get lost on the Internet.

We stay safe and only open emails from people that we know.

We never tell anyone on the internet our Name, email address, telephone number or where we live. It might not be the person we think it is!

We have completed the BBC e-Safety training for kids.