

July 2015



E-Safety Policy

Agreed at: _____

Signed _____

Date _____

Contents

1.	Introduction/Aims.....	3
2.	What does an i-confident child look like at Summerhill	4
3.	Email use, Social Networking sites, monitoring and management.....	5
4.	How will misuse at Summerhill be addressed.....	6
5.	Summerhill Academy E safety agreement.....	7

E-Safety Policy

Summerhill Academy E-safety

Policy For Acceptable Use

Introduction

Use of the internet is an integral part of the learning process at Summerhill Academy. Whilst the internet offers many benefits and opportunities across the curriculum, its use necessitates the need for a clear policy on how the internet should be used safely. This document aims to set out high-level guidelines to help ensure that children are safe whilst using the internet.

What is the aim of the e-safety and acceptable use policy?

Pupils interact with new technologies such as mobile phones, play-stations, I-pads and the internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial, however can occasionally place young people in danger.

As a school, it is part of our duty of care to ensure that we educate our children about the safe use of technology. They need to be aware of potential dangers and problems that they may come across whilst using technology and be able to deal with them in a confident, mature manner. We want to strike a balance between controlling access, setting rules and educating our students for responsible use.

At Summerhill Academy we believe that we can do this by helping our children to be internet confident.

What does an i-confident child look like at Summerhill Academy?

- They will challenge information presented to them.
- They show an awareness that not all sources on the internet are correct or useful, for example, do they know that the Google links come up in order of popularity not truthfulness?
- They have some awareness of internet scams.
- They understand that some sites have agendas.
- They understand the importance of a positive online identity.
- They protect their online image by careful vetting of images and text.
- They recognise that information presented online is difficult and sometimes impossible to remove once posted.
- They realise that text without facial expressions and sound context can be misunderstood.
- They understand the importance of tailoring information to the audience.
- They protect each other.
- They report cyber bullying, both when it is happening to them and when they see it happening to someone else.
- They coach and support their peers in making good, sound online decisions.
- They are confident in discovering new things.
- They look for ways to use new technologies to present work, share information and communicate effectively.
- They discover and evaluate new technologies considering the benefits to them, the disadvantages and the safety risks.
- They evaluate risks in technology.
- They weigh up possible benefits against likely dangers, particularly applicable for open chat rooms and social networking sites.
- They know how to reduce the risks involved, for example, real friend's only, locked profile and don't share passwords or usernames.
- They show awareness of viruses by understanding that internet sites and emails can carry viruses. Be aware of anti-virus software and its purpose.
- They know that not all emails are trustworthy and that they should only open an email if they trust the source. Begin to show an awareness of verification of the source.
- They know what technology can and can't do.
- They understand that technology isn't the only source available to use as a resource.

Practical guidelines for safe internet use by teachers

Teachers should evaluate any websites fully **before** they use them with their pupils. Often this means checking the websites, search results etc just before the lesson. What may be considered a safe site today might not be tomorrow. Teachers need to pay particular attention to image advertisements as they can change each time the web page is accessed.

How will pupils learn to evaluate internet content?

E-safety should be incorporated across all aspects of the computing curriculum and integrated into all appropriate lessons. Teachers have a responsibility to educate children on both the dangers and restrictions of the internet during computing and PSHE sessions. This will begin to be introduced across certain units of work and monitored by phase leaders, the Computing leader and the PSHE leader.

The use of E-mail

Pupils may only use approved e-mail accounts on the school system. If a pupil receives an offensive email, they must inform their teacher immediately. In e-mail communication, pupils must not reveal their personal details or those of others. Children will be taught to treat all incoming mail as suspicious. They will be taught to only open emails from addresses they recognise and told not to open attachments unless the author is known. Children will be made aware that the forwarding of chain letters is not permitted and will be both categorised and treated as inappropriate use of the internet.

Social Networking Sites

Summerhill Academy currently controls access to social networking sites and they are not available through the school internet. However, pupils are advised never to give out personal details of any kind which may identify them, their friends or their location. Parents and pupils will be advised, through the computing and PSHE curriculum, that the use of social networking sites outside school brings a range of dangers to primary school children. Pupils will be encouraged to use safer networking areas. It is important that we recognise the children's current interest in such sites and educate them accordingly on the dangers and legal age limits e.g. The age limit for a child to use Facebook is 13 so primary aged children should not be accessing the site, although the Academy are aware that children under the age of 13 at Summerhill are accessing it.

How will use of the internet be monitored and managed?

At Summerhill Academy our internet connection incorporates a filtering system or "firewall" appropriate to the age of our pupils which screens undesirable sites at a proxy server. However, it is impossible to filter all sites and that is why e-safety education is vital across the curriculum. As an extra precaution, all teachers have a responsibility to monitor the range of sites used and should pre-plan sites to be used with the children and sites used to download materials onto the network. Any concerns over websites should be reported to the SLT immediately so that they can be passed on to the Cabot ICT team who can deal with these concerns accordingly. Teachers should only recommend websites to children, particularly for home use, that they have accessed themselves and know are safe to be used by primary aged children. Antivirus software is monitored regularly by the Cabot ICT team and technicians and is installed on all computers throughout the school. Children will be taught to inform a member of staff if they are concerned about the appropriateness of the site.

Acceptable User Agreements

To ensure that staff, parents and pupils are aware of the e-safety rules, each will be issued with an acceptable user agreement. Everyone must read the guidelines set out and sign to confirm their acceptance. Parents and Pupils will be sent the acceptable user agreement for pupils. Parents are expected to share this with their children and ensure that they fully understand the guidelines set out. Both parent and child must sign this agreement to confirm their acceptance. The acceptable user agreements will also be discussed in computing lessons and PSHE lessons when teaching something of relevance to strengthen the children's awareness of each statement in the agreement. Please find the acceptable user agreements at the end of this policy.

How will misuse of the internet at Summerhill Academy be addressed?

Misuse of the Internet will **not be tolerated** at Summerhill. In the first instance, the class teacher should deal with any misuse of the internet with the child and inform the parents. However, the incident must always be reported to the SLT and recorded in writing to provide a record on the 'Safeguarding Record Of Concern' forms which can be located in the office of the Safeguarding lead. Should there be any concerns over the types of material accessed; the matter should immediately be reported to the principal who will ensure that appropriate action is taken. The sanctions imposed will reflect the severity of the incident and follow the school's behavioural policy. Pupils must report accidental access to inappropriate material immediately to their teacher, who will then inform the SLT.

Good E-Safety websites to use with children

E-Safety Driving License <http://pbskids.org/license/index.html>

Hector's World http://www.thinkuknow.co.uk/5_7/default.aspx

Think you know (8-10 years old) http://www.thinkuknow.co.uk/8_10/

More mature children <http://www.chatdanger.com>

This policy will be updated in line with advances in technology.

Our Summerhill Academy nominated E-Safety Officer is: Kirstie McLeod

Policy written: July 2015

Policy approved by Academy Council: July 2015

Policy review: April 2017

Summerhill Academy E-safety Acceptable User Agreement

Use of the internet is an integral part of the learning process at Summerhill Academy. Whilst the internet offers many benefits and opportunities across the curriculum, its use necessitates that children, teachers, parents and carers should all understand how to use the internet safely. As a school, it is part of our duty of care to ensure that we educate our children about the safe use of technology. They need to be aware of potential dangers and problems that they may come across whilst using technology and be able to deal with them in a confident, mature manner.

We are asking all parents and carers to go through the points below with their children to ensure that they fully understand the guidelines set out:

- Children should not share personal information such as their name or address on the internet.
- Children should not say anything to anyone on the internet that they wouldn't say to someone's face or that could be unkind – creating a positive online identity.
- Children should not arrange a face to face meeting with someone they have 'met' online.
- Children will challenge information presented to them.
- Children will show an awareness that not all sources on the internet are correct.
- Children realise that text without facial expressions and sound can be misunderstood.
- Children protect each other e.g. they report cyber bullying, both when it is happening to them and when they see it happening to someone else.
- Children coach and support their peers in making good, sound online decisions.
- Children are confident in discovering new things.
- Parents should monitor and engage with their children about what they are doing online.
- Parents should think to use filtering systems that will block unsuitable content.
- Parents should be supportive and approachable and make sure their children know they can talk to them should something go wrong online.
- Parents explain to children that their 'digital footprint' can be seen by schools, universities, colleges and employers in the future so it is important to be careful now.

Misuse of the Internet will **not be tolerated** at Summerhill. In the first instance, the class teacher will deal with any misuse of the internet with the child and inform the parents. However, the incident must always be reported to the principal and recorded in writing to provide a record.

For any further information that you require concerning e-safety at Summerhill Academy please see the e-safety policy available on our Summerhill website.

Summerhill Academy E-safety Acceptable User Agreement

Once you have read the guidelines with your child please return this tear off slip signed and dated.

I (child) understand the e-safety guidelines set out.

Signed: _____ Date: _____

I (parent/carer) have gone through the e-safety guidelines with my child.

Signed: _____ Date: _____