Roundthorn Primary Academy

E-Safety & Acceptable Use Policy

March 2012

Updated: July 2012

Agreed by Staff

Agreed by Governing Body .....

E-SAFETY POLICY – 1

Introduction

- This document is a statement of the aims and effective approaches to e-safety at Roundthorn.
- It was developed during the Spring 2012 through a process of Consultation with staff and governors and the Sanctuary ict collaborative.
- Safeguarding children, including e-safety is everyone's responsibility.

What is e-safety?

The term 'e-safety' is used to encompass the safe use of all on-line technologies in order to protect pupils from potential and known risks.

Aims

The focus of this policy is to clarify the roles, responsibilities and procedures for the acceptable, safe and responsible use of on-line technologies and to ensure that existing policies (such as those on child protection, bullying, the curriculum, and behaviour) are applied to the digital environment. In order for this to happen, it is essential that these policies are regularly reviewed against this e-safety guidance, and updated as necessary.

This policy covers:

•Managing on-line technology so that children are kept as safe as possible.

•The responses necessary when a risk to a child is discovered.

Managing the use of on-line technology

The E-safety Lead

At Roundthorn School the e-safety leads are the ict coordinator and Andrew Hulmes (who is also one of the designated child protection officers.) The responsibilities of the lead person include:

- •Updating the E-Safety and Acceptable Use Policy.
- •Ensuring that policies and procedures include aspects of e-safety for example the anti-bullying procedure includes cyber-bullying. Child protection policy to include Internet grooming.
- Work with the IT technician provider to ensure that the filtering is set at the correct level for staff and children.
- Ensure staff training is provided on e-safety issues
- Ensure e-safety is included in staff induction
- Monitor and evaluate incidents that occur to inform future safeguarding developments

Principles of the Teaching and Learning of e-safety

The purpose of using on-line technology in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

The school Internet access is designed expressly for pupil use and includes filtering

appropriate to the age of pupils.

In addition to accessing the Internet at Roundthorn, we recognise that children will use the Internet and other digital technology in their own time at other locations and are at greater risk **if** they have not been taught what the dangers are and how to use them safely. Supporting and assisting the development of childrens' e-confidence and their ability to access the digital world effectively and safely is essential.

We acknowledge that the range of risks to young people in the digital environment is wide and ever-changing e.g 'Grooming' by sexual predators via Internet-enabled multi-player games is not uncommon.

At Roundthorn we recognise the importance of raising the awareness of children so that they are able to keep themselves as safe as possible when using the Internet and other digital technologies. In order to do this, we involve children and their parent / carers in the safe use of on-line technologies. Children are taught what on-line technology use is acceptable and what is not and given clear objectives for its use. Children are educated in the effective use of on-line technology in research, including the skills of knowledge location, evaluation and retrieval. Lessons on e-safety are also delivered and local PCSO's provide input and scenarios regarding e-safety for the children to consider.
We support the Oldham Charter of Young People's Digital Rights because a key element of child protection in the digital environment is developing the skills and confidence of young people in the face of threats to their safety, enabling them to adopt the safest possible behavior's themselves and to be able to report situations and behaviors of others that could constitute a threat. These messages are more likely to be adopted and taken to heart by children if presented in terms of their own rights than if presented as a set of rules about what they shouldn't do. (See appendix 1.)

We provide support and guidance to pupils and their parents/carers for the safe and responsible use of these on-line technologies. A partnership approach with parents is encouraged and guidance regarding e-safety is offered to parents in a variety of different ways e.g. information evenings, relevant links and documents available on the school website. (See appendix 2 for a list of websites that contain useful information and resources about e-safety.)

Acceptable Use
In order to prevent inappropriate situations occurring it is important that staff, volunteers and children are aware of their responsibilities and the expectations whilst using technology. Each user signs a contract to ensure that they know what is deemed 'acceptable use of the Internet'. (Please see appendices 3&4).

Password security
Password security is essential for staff, as they are able to access and use pupil data. Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks and MIS. Staff should ensure that computers and laptops are not left unattended.

Internet access

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils. Internet access is planned to enrich and extend learning activities. Parents of all pupils are asked to sign and return a consent form giving permission for their child to use the Internet.
In Foundation Stage and Key Stage 1, access to the Internet is by adult demonstration and direct supervised access to specific, approved on-line materials.
In Key Stage 2, pupils use the Internet for research purposes in addition to specific tasks. Pupils are taught the importance of e-safety and agree terms and conditions for acceptable Internet use. Pupils are taught to be critically aware of the materials they read and are made aware that information may be not always be reliable or accurate.
Many young people, volunteers and staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through various acts (See appendix 6).

Email

Children may only use approved email accounts on the school system. Children use class accounts that are restricted to communication within the school, within the schools virtual learning environment. Children must not reveal details of themselves or others in email communication, such as address or telephone number, or arrange to meet someone. Children are instructed to tell an adult if they receive an offensive email. Email sent to external organisations should be carefully written and authorized before sending, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.

School Website

The point of contact on the website should be the school address, school email and telephone number. Staff or pupils' home information will not be published. Website photographs that include pupils will be selected carefully. Pupils' full names will not be used anywhere on the website, particularly in association with photographs. Written permission from parents/carers will be obtained before photographs of pupils are published on the school website.

Chat and instant messaging

Staff and pupils will not be allowed access to public or unregulated chat rooms. Pupils will not access social networking sites e.g. 'My space', 'Bebo', 'facebook'. Pupils will only be allowed to use regulated educational chat environments, such as those in the VLE. This will be supervised and the importance of chat room safety emphasized. Any forms of bullying or harassment is strictly forbidden.

Photographic, video and audio technology

When not in use video conferencing cameras should be switched off and turned to face the wall. It is not appropriate to use photographic or video devices in changing rooms or toilets. Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed. Staff may use photographic or video devices (including digital cameras and mobile phones) to support school trips and curriculum activities. The downloading of audio and video files is not permitted, without the prior permission of the e-safety lead and only in cases where they relate directly to the

current educational task being undertaken. Pupils should always seek the permission of their teacher before making audio, photographic or video recordings within school grounds.

Mobile phones
Children must not bring mobile phones into school. Staff must have their mobile phones on 'silent' during teaching times and these must be kept in a locked unit when not in use. Staff must not have mobile phones in there contact when working with small groups. The sending of abusive or inappropriate text messages is strictly forbidden as is the use of mobile phones to take pictures or videos.

Emerging ICT applications
Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. At Roundthorn Emerging applications such as the use of Ipods and Ipads are encouraged, and will be used in accordance to this policy.

Assessment of risk
In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Oldham LA can accept liability for the material accessed, or any consequences of Internet access. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. Methods to identify, assess and minimise risks will be reviewed regularly. The headteacher will ensure that the E-safety and Acceptable Use Policy is implemented and compliance with the policy monitored.

Filtering
The school will work in partnership with parents, the LA, DCSF and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. See appendix 5 for procedures when material that the school believes is illegal is discovered. The filtering strategy is selected to suit the age and curriculum requirements of the pupils.

Introducing the policy to pupils
- Rules for acceptable use will be posted in all rooms where computers are used.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- A module on responsible Internet use will be included in the PSHE programme covering both school and home use.
- Oldham's youth charter will be displayed. (See appendix 1)

Introducing the policy to staff and volunteers
- All staff and volunteers must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.

•All staff including teachers, supply staff, classroom assistants, administration and caretaking staff, and Governors will be provided with the School Internet Policy, and its importance explained.
•Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
•The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
•Staff development in safe and responsible Internet use, including familiarisation of the E-safety and acceptable use policy will be provided as required.

Maintaining ICT system security
•The school ICT systems will be reviewed regularly with regard to security.
•Virus protection will be installed and updated regularly.
•Security strategies will be discussed with the Sanctuary ICT Collaborative.
•Personal data sent over the Internet will be encrypted or otherwise secured. All personal devices will be encrypted by the ICT team.
•Each teaching staff member has been given a personal portable USB device which is encrypted with password protection, this allows for safe use.
•Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
•Files held on the school's network and the cloud will be regularly checked.
•The ICT co-ordinator / ICT technicians will ensure that the system has the capacity to take increased traffic caused by Internet use.

The responses necessary when a risk to a child is discovered.

Prompt action is required if a complaint is made regarding the use of on-line technology. The facts of the case must be established and presented to the e-safety lead. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could be potentially more serious and a range of sanctions will be used, linked to the Behaviour Policy. Complaints of a child protection nature will be dealt with in accordance with Oldham LSCB child protection procedures.

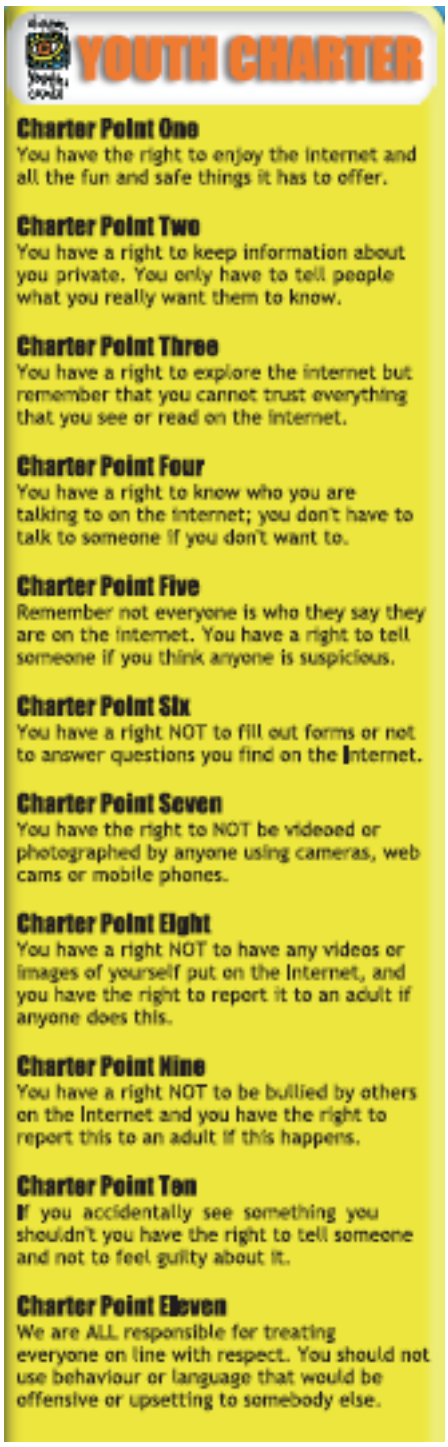
Any complaints about staff misuse of on-line technology must be referred directly to the headteacher.

See appendix 5 for procedures to be adhered to in the event of any misuse of the Internet.

REVIEW OF POLICY:

This policy will be reviewed in line with the Policy Management Cycle.

Appendix 1-Oldham Charter of Young People's Digital Rights



YOUTH CHARTER

Charter Point One
You have the right to enjoy the internet and all the fun and safe things it has to offer.

Charter Point Two
You have a right to keep information about you private. You only have to tell people what you really want them to know.

Charter Point Three
You have a right to explore the internet but remember that you cannot trust everything that you see or read on the internet.

Charter Point Four
You have a right to know who you are talking to on the internet; you don't have to talk to someone if you don't want to.

Charter Point Five
Remember not everyone is who they say they are on the internet. You have a right to tell someone if you think anyone is suspicious.

Charter Point Six
You have a right NOT to fill out forms or not to answer questions you find on the Internet.

Charter Point Seven
You have the right to NOT be videoed or photographed by anyone using cameras, web cams or mobile phones.

Charter Point Eight
You have a right NOT to have any videos or images of yourself put on the Internet, and you have the right to report it to an adult if anyone does this.

Charter Point Nine
You have a right NOT to be bullied by others on the Internet and you have the right to report this to an adult if this happens.

Charter Point Ten
If you accidentally see something you shouldn't you have the right to tell someone and not to feel guilty about it.

Charter Point Eleven
We are ALL responsible for treating everyone on line with respect. You should not use behaviour or language that would be offensive or upsetting to somebody else.

Appendix 2 Information and websites about e-safety.

CEOP

- http://www.ceop.gov.uk

Think U Know

- http://www.thinkuknow.co.uk/Default.aspx?AspxAutoDetectCookieSupport=1

Becta

- http://localauthorities.becta.org.uk/index.php?section=esf

Childnet

- http://www.childnet-int.org

Internet Watch Foundation

- http://www.iwf.org.uk

BBC

- http://www.bbc.co.uk/cbbc/help/web/staysafe

Appendix 3 Contract for Acceptable Use of the Internet (Staff/volunteer)

I know that I should only use school equipment in an appropriate manner.

I know that images should not be inappropriate or reveal any personal information of children and young people if uploading to the Internet.

I have read the school e-safety and acceptable use policy so that I can deal effectively with any problems that may arise.

I will report accidental misuse to the headteacher.

I will report any incidents of concern for the children's safety to the headteacher, designated person for child protection in accordance with the e-safety and acceptable use policy.

I know who the designated person for child protection is.

I will ensure that personal data (such as data held on SIMS) is kept secure.

I will ensure that no data is stored without the use of my personal USB encrypted device.

I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.

I will ensure that al electronic communications with pupils and staff are compatible with my professional role.

Name: ……..

Signed: ……..

Position: ……..

Date: ……..

Appendix 4 Contract for Acceptable Use of the Internet (Pupil)

Rules for Responsible Internet Use

Pupils

The school has computers and internet access to help our learning. These rules will keep everyone safe and help us be fair to others.

- I will only access the email with my own login and password, which I will keep secret;

- I will not access other people's files;
- I will only use the computers for school work and homework;
- I will not bring CD's or a memory stick into school;
- 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 use our Virtual Learning environment and our new technologies such as ipads and Ipods safely.

- The messages I send will be polite and sensible;
- I will not give my home address, telephone number, email address or personal website details, or arrange to meet someone, unless my parent, carer or teacher has given permission;
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;
- I understand that the school may check my computer files and may monitor the internet sites and Apps I use.

Appendix 5 How to respond if a risk is discovered

The E-safety lead will ensure that an adult follows these procedures in the event of any misuse of the Internet:

An inappropriate website is accessed inadvertently:

- Report website to the e-safety lead.
- Contact the filtering service so that the site can be added to the banned or restricted list.

•Change Local Control filters to restrict locally.
•Log the incident.

An inappropriate website is accessed deliberately:
•Ensure that no one else can access the material by shutting down the computer.
•Log the incident.
•Report to the Headteacher and e-Safety lead immediately.
•Headteacher to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
•Inform the filtering services in order to reassess the filters.

An inappropriate website is accessed deliberately by a child or young person:
•Refer the child to the Acceptable Use Rules that were agreed.
•Reinforce the knowledge that it is illegal to access certain images and police can be informed.
•Log the incident.
•Decide on appropriate sanction.
•Notify the parent/carer.
•Contact the filtering service to notify them of the website.

An adult receives inappropriate material:
•Do not forward this material to anyone else – doing so could be an illegal activity.
•Alert the Headteacher immediately.
•Ensure the device is removed and log the nature of the material.
•Contact relevant authorities for further advice e.g. police, social care CEOP.
•Log the incident

An illegal website is accessed or illegal material is found on a computer.
(The following incidents must be reported directly to the police):
•Indecent images of children found. (Images of children whether they are or cartoons of children or young people apparently under the age of 16, involved in sexual activity or posed in a sexually provocative manner)
•Incidents of 'grooming' behaviour.
•The sending of obscene materials to a child.
•Criminally racist or anti-religious material
•Violent or bomb-making material
•Software piracy
•The promotion of illegal drug-taking
•Adult material that potentially breaches the obscene publications act in the UK.

If any of these are found, the following should occur:
•Alert the manager / e-safety lead immediately.
•**DO NOT LOG OFF** the computer but disconnect from the electricity supply.
•Contact the police and or CEOP and social care immediately (Police - 0161 856 8962, social care -0161 770 3790, children over 16 - 0161 770 6599, out of hours – 0161

770 6936).
If a member of staff or volunteer is involved, refer to the allegations against staff policy and report to the Local Authority Designated Officer.

An adult has communicated with a child or used ICT equipment inappropriately (e-mail/ text message etc)
•Ensure the child is reassured and remove them from the situation.
•Report to the manager and Designated Person for Child Protection immediately, who
will then follow the Allegations Procedure and Child Protection Procedures www.oldham.gov.uk/lscb-home .
•Report to the Local Authority Designated Officer (0161 770 8870).
•Preserve the information received by the child if possible.
•Contact the police as necessary.

Threatening or malicious comments are posted to the school website or learning platform (or printed out) about an adult in school:
•Preserve any evidence and log the incident.
•Inform the Headteacher immediately and follow Child Protection Policy.
•Inform the e-Safety Leader so that new risks can be identified.
•Contact the police or CEOP if appropriate.

Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to the Headteacher.

Threatening or malicious comments are posted to the school website or learning platform about a child in school or malicious text messages are sent to another child/young person (cyber bullying).
•Preserve any evidence and log the incident.
•Inform the manager immediately.
•Check the filter if an Internet based website issue.
•Contact/parents and carers.
•Refer to the bullying policy.
•Contact the police or CEOP as necessary

Appendix 6 Legal Framework

This section is designed to inform users of legal issues relevant to the use of Communications. It is not professional advice.

The Sexual Offences Act 2003,
•The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an Offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.
•Causing a child under 16 to watch a sexual act is illegal, including looking at images, such as videos, photos or web cams, for your own gratification.
•It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category

of trust).
•Any sexual intercourse with a child under the age of 13 commits the offence of rape.
•More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)
•Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment.
•This wording is important because an offence is complete as soon as the message has been sent, there is no need to prove any intent or purpose.

Data Protection Act 1998
•The Act requires anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)
•Regardless of an individual's motivation, the Act makes it a criminal offence to: lgain access to computer files or software without permission (for example using someone else's password to access files); gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or impair the operation of a computer or program (for example caused by viruses or denial of service attacks).
•UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)
•This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
•Copyright is the right to prevent others from copying or using his or her "work" without permission.
•The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer.
•It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material.
•It is also illegal to adapt or use software without a licence or in ways prohibited by

the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)
•This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material, which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)
•It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
•Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
•A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
•A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000
•The Regulation of Investigator Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998.
•The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored.
•Covert monitoring without informing users that surveillance is taking place risks Breaching data protection and privacy legislation.