RAINFORD CHURCH OF ENGLAND PRIMARY SCHOOL

School, church and community working together'

E-Safety and Acceptable Use Policy

For approval by Full Governors: 24th November 2015

To be reviewed on or before: Autumn 2017

Signed…… Chair of Governors

Signed…… Headteacher

Rainford CE Primary School E- Safety Policy

Our e-Safety Policy has been written by the school following government guidance. It has been agreed by the Leadership Group and approved by governors. The E-Safety Policy is part of the ICT Policy and School Development Plan and relates to other policies including those for behaviour, personal, social and health education (PSHE).

The E-Safety Policy and its implementation will be reviewed annually.

Introduction

ICT in the 21st Century is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to arm our young people with the skills to access lifelong learning and employment. Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. 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
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Rainford CE Primary School, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Teaching and Learning

The purpose of Internet use 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 functions. Internet use is part of the statutory curriculum and a necessary tool for learning. Internet access is an entitlement for pupils who show a responsible and mature approach to its use. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Internet use to benefit education

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments,
- educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with St Helens Council and DfE;
- access to learning wherever and whenever convenient

Internet use to enhance learning

The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Evaluation of Internet content

The schools will ensure that the copying and subsequent 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. Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work. The evaluation of on-line materials is a part of every subject.

PREVENT DUTY

This school takes seriously its duty contained in the Counter Terrorism and Security Act (2015) to prevent pupils and those working in school from being radicalised or drawn into extremism. We will follow the advice contained within the new statutory guidance on the legal duty set out in the 'Prevent Duty Guidance: For England and Wales (2015)' in conjunction with the other duties which we already have for keeping pupils safe.

<u>Managing Information Systems</u>

Security of Information System

The security of the school information systems will be reviewed regularly.

Virus protection will be updated regularly.

Portable media, i.e. pen sticks, CDR and DVDs, may not be used without specific permission followed by a virus check. Sensitive data must not be removed from school via portable memory device.

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 will be regularly checked.

The ICT co-ordinator / network manager will review system capacity regularly.

The school may save pupils' work to 'Dropbox' which is password protected. Passwords should contain a mixture of capitals and figures and should not be related specifically to the school, teacher or pupils.

E-Mail Use

Pupils may only use approved e-mail accounts related to our learning platform.

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.

Access in school to external personal e-mail accounts may be blocked.

Excessive social e-mail use can interfere with learning and may be restricted.

E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

The forwarding of chain letters is not permitted.

Management of Published Content

The contact details on the website are the school address, e-mail and telephone number.

Staff, governors or pupils' personal information must not be published.

E-mail addresses should be published carefully, to avoid spam harvesting.

The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.

Images 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 website, particularly in association with photographs.

Written permission from parents or carers must be obtained before images of pupils are electronically published.

Work can only be published with the permission of the pupil and parents.

Management of social networking and personal publishing

The schools will block/filter access to social networking sites and Newsgroups.

Pupils will be advised that when using these sites from home they should never give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, e-mail addresses, full names of friends, specific interests and clubs etc.

Pupils should be advised not to place personal photos on any social network space. Advice should be given regarding background detail in a photograph which could identify the pupil or his/her location e.g. house number, street name or school.

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.

Pupils should be advised not to publish specific and detailed private thoughts or actions.

Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Management of the filtering system

The school will work with Agylysis and the Local Authority to ensure that systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL must be reported to the ICT Coordinator who will take appropriate action. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that the school believes is illegal must be reported to appropriate agencies such as IWF or CEOP. Agylysis has control over the blocking and unblocking of certain sites. Any request to unblock will be reviewed before completion.

Management of Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Pupils who have specific circumstances that require access to a mobile phone, prior to and after the end of the school day, MUST hand it in to the office on arrival and collect it at the end of the day.

Protection of Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Policy Decisions

Authorisation of Internet Access

The school will maintain a current record of all staff, governors and pupils who are granted access to the school's electronic communications.

All staff, governors and visitors must read and sign the acceptable usage policy before using the school network.

All pupils from KS1 and KS2 must read and agree to an acceptable usage policy.

At Key Stage 1, access to the Internet will be by adult demonstration and directly supervised access to specific, approved on-line materials.

Parents will be informed that pupils will be provided with supervised Internet access

Risk Assessment

The school will take all reasonable precautions to ensure that users access only appropriate material. (See Management of the filtering system). However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor St Helens Council can accept liability for the material accessed, or any consequences resulting from Internet use.

The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

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.

Handling of e-safety complaints

Complaints of Internet misuse (including social networking concerns) will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to one of the ICT subject leaders, who in turn may refer this to the Senior Leadership Team. Pupils and parents will be informed of the complaints procedure. Parents and pupils will need to work in partnership with staff to resolve issues.

Sanctions may include:

- A temporary or permanent ban on Internet use.
- Suspension of online learning site logins
- Additional disciplinary action may be added in line with the school's behaviour policies.
- Where applicable, parents and other external agencies may be contacted.

Use of the Internet across the community

The school will liaise with local organisations to establish a common approach to e-safety. The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

Use of digital images

When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

• In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents / carers comment on any activities involving staff or other pupils in the digital / video images.

• Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff or volunteers should not be used for such purposes.

• Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

• Pupils must not take, use, share, publish or distribute images of others without their permission.

• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

• Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. This is covered as part of the Acceptable Use Agreement (AUA) signed by parents or carers at the start of the year - see Parents / Carers Acceptable Use Agreement in the appendix)

• Pupil's work can only be published with the permission of the pupil and parents or carers.

Communications Policy

Cyber Bullying

Cyber bullying is the use of ICT, particularly mobile phones and the internet, deliberately to upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head teachers have the power; 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site. Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example menacing and threatening communications (Please see the school's Anti-Bullying Policy). There are many types of cyber-bullying. Here are some of the more common:

1. Text messages —that are threatening or cause discomfort - also included here is "bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology)

2. Picture/video-clips via mobile phone cameras - images sent to others to make the victim feel threatened, upset or embarrassed.

3. Mobile phone calls — silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.

4. Emails — threatening or bullying emails, often sent using a pseudonym or somebody else's name.

5. Chatroom bullying — menacing or upsetting responses to children or young people when they are in web-based chatroom.

6. Instant messaging (IM) — unpleasant messages sent while children conduct real-time conversations online using Chat

7. Bullying via websites — use of defamatory blogs (web logs), personal websites and online personal "own web space" sites such as Bebo and MySpace.

The best way to deal with Cyberbullying is to prevent it happening in the first place and to have clear steps to take when responding to it

Preventing Cyber Bullying

It is important that we work in partnership with pupils and parents, educating them about Cyberbullying; as part of our e-safety curriculum.

They should:

• understand how to use these technologies safely and know about the risks and consequences of misusing them

• know what to do if they or someone they know are being cyber bullied.

• report any problems with Cyberbullying. If they do have a problem, they can talk to school staff, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP) to do something about it.

Additional online advice on how to react to Cyberbullying can be found on www.kidscape.org and www.wiredsafety.org

Introduction of e-safety to pupils

E-Safety rules will be posted in rooms with Internet access.

E-safety information will be displayed in a prominent place in school.

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

The e-safety rules will be revisited annually, as part of the PSHE and ICT curriculum to raise the awareness and importance of safe and responsible internet use both in school and at home

Instruction in responsible and safe use should precede Internet access.

The ICT Co-ordinator will deliver Internet Safety Assemblies for KS1 and KS2(separately) once each term.

Discussion of e-safety policy with staff

All staff will be given the School e-Safety Policy and its application and importance explained.

Staff should be aware that Internet traffic can be monitored and traced to the individual user.

Discretion and professional conduct is essential.

Staff that manage filtering systems or monitor ICT use will be supervised by the Senior Leadership Team and have clear procedures for reporting issues.

Staff training in safe and responsible Internet use and on the school e-safety Policy will be provided as required.

Parent Support

Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school prospectus and on the school website.

Internet issues will be handled sensitively, and parents will be advised accordingly.

A partnership approach with parents will be encouraged.

Interested parents will be referred to organisations listed below under e-Safety Contacts and References

e-Safety Contacts and References

BBC Chat Guide -http://www.bbc.co.uk/chatguide/

Becta -http://www.becta.org.uk/schools/esafety

Childline -http://www.childline.org.uk/

Child Exploitation & Online Protection Centre -http://www.ceop.gov.uk

Grid Club and the Cyber Café -http://www.gridclub.com

Internet Watch Foundation -http://www.iwf.org.uk/

Internet Safety Zone -http://www.internetsafetyzone.com/

Kidsmart -http://www.kidsmart.org.uk/

NCH – The Children's Charity -http://www.nch.org.uk/information/index.php?i=209

NSPCC -http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Stop Text Bully -www.stoptextbully.com

Think U Know website -http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse -http://www.virtualglobaltaskforce.com/

Notes on the legal framework

This section is designed to inform users of legal issues relevant to the use of communications. It is not professional advice. Many young people and indeed some 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:

The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the child to 18 years old;

The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and l The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening.

Other laws already protect people from threats based on their race, nationality or ethnic background.

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 webcams, 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).

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: gain 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 pseudophotographs (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 Investigatory 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.

Equality Act 2010

We as a school community have a commitment to promote equality. Therefore, an equality impact assessment has been undertaken and we believe this policy is in line with the Equality Act 2010.

Appendix 1

Rainford CE Primary School - Acceptable Use of ICT Agreement -Staff, Governor and any Visitors who may use any ICT equipment, technology or mobile devices whilst on school premises.

Acceptable Use Agreement / Code of Conduct

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff, governors or visitors are aware of their professional responsibilities when using any form of ICT. All staff, governors or visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Miss Tose or Mr Attrill, the school ICT coordinators.

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 Head or Governing Body.

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 email address, to pupils.

I will only use the approved, secure email system(s) for any school business (staff members only).

I will ensure that personal data (such as data held on SIMS) 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 Head or Governing Body.

I will not use or install any hardware (including USB sticks) or software without permission from the ICT subject leader.

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, stored and used for professional purposes inline 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 Head teacher.

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 by the Head teacher.

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.

I will ensure that only children whose parents have given permission for them to use the Internet and ICT are enabled to do so at school.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school

Signature …… Date ……

Full Name ……

Appendix 2

Acceptable Usage Policy KS1 Children – Linked to 360 Safe AUP Guidelines

These rules have been written to make sure that you stay safe when using the computers.

This includes cameras, laptops, I-Pads and webcams. By using the ICT in school, you have agreed to follow these rules. Your teacher will talk about these rules before you sign them and a copy will be sent home to your parents.

If you have any questions, please ask your teacher, Miss Tose or Mr Attrill

The Golden Rule: Think before you click

I will be careful when going on the internet

I will only use the internet when a teacher is with me

I will tell a teacher if I see something that upsets me

I know people online might not be who they say they are

I will be polite when talking to people or writing online

I will think before I print or delete

I will be careful when using or carrying equipment

I will keep my password secret, but I can tell my family

I will remember to log off properly

I will handle all computer equipment with care

I won't tell anyone any personal details like my phone number, address or last name

I won't log on the learning platform using someone else's username

I will never put water bottles on the table when using ICT equipment

Signed (Pupil)_____Class:_____Date: _____

Appendix 3

Acceptable Usage KS2 Children – Linked to 360 Safe AUP Guidelines

These rules have been written to make sure that you stay safe and act responsibly when using the computers. When we talk about ICT, we are talking about computers, laptops, netbooks, and everything including cameras, web cams, I-Pads and tablets. These rules will have been discussed in class and a copy sent home to your parents.

If you have any questions, please ask your teacher, Miss Tose or Mr Attrill

Keeping Safe

I will not use ICT in school without permission from my teacher

I will be careful when going on the internet. I will log off sites when I have finished

I must keep my personal details and those of others private

At all times, I will think before I click (especially when deleting or printing)

I know that teachers can, and will, check the files and websites that I have used

I will keep my usernames and passwords secure, but I understand that I can share them with appropriate people, such as my parents or teachers

Communicating

When communicating online (in blogs, emails, forums etc) I will think about the words that I use and will not use words that may offend other people. I know that I need to be polite and friendly online

I am careful about what I send as messages as they can they can viewed by the ICT co-ordinators and Headteacher

When communicating online I will only use my first name and not share personal details such as my email address, address or phone number

I understand that people online might not be who they say they are

If an online friend wants to meet me I will tell an adult. I will NEVER arrange to meet anyone without permission.

I will not log on the learning platform using another child's account

I will NOT contact any member of staff via any social networking site

Research and Fun

When using the internet, I will think about the websites that I am accessing

I will use clear search words so that I find the right information

When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site

Sharing

I will not look at other people's files or documents without their permission

I will not install any software or hardware (including memory sticks) or try to change computer settings without permission from the teacher

I will not take or share pictures of anyone without their permission

I know that anything I put up on the internet can be read by anyone

Problems

If I find a website, image or message that is inappropriate, I will tell my teacher straight away

I will take care when using the computers and transporting equipment around. I will tell a teacher if equipment is broken or not working

I understand that if I am acting inappropriately then my parents may be informed and access to the learning platform may be suspended

Signed (Pupil)_____Class:_____Date:_____

Appendix 4

Rainford CE Primary School E Safety Incident Log

Details of ALL e-safety incidents to be recorded in the Incident Log by the ICT Subject Leader.

This incident log will be monitored termly by the SLT and Head teacher.

Date/Time	Name of Pupil or Staff	Male/ Female	Room and computer device	Details of Incident	Actions and Reasons

Appendix 5

Advice for Children on Cyber-bullying

If you're being bullied by phone or the Internet

• Remember, bullying is never your fault. It can be stopped and it can usually be traced.

• Don't ignore the bullying. Tell someone you trust, such as a teacher or parent, or call an advice line.

• Try to keep calm. If you are frightened, try to show it as little as possible. Don't get angry, it will only make the person bullying you more likely to continue.

• Don't give out your personal details online - if you're in a chatroom, watch what you say about where you live, the school you go to, your email address etc. All these things can help someone who wants to harm you build up a picture about you.

• Keep and save any bullying emails, text messages or images. Then you can show them to a parent or teacher as evidence.

• If you can, make a note of the time and date bullying messages or images were sent, and note any details about the sender.

There's plenty of online advice on how to react to cyberbullying. For example, www.kidscape.org and www.wiredsafety.org have some useful tips: Text/video messaging You can easily stop receiving text messages for a while by turning off incoming messages for a couple of days. This might stop the person texting you by making them believe you've changed your phone number. To find out how to do this, visit www.wiredsafety.org.

• If the bullying persists, you can change your phone number. Ask your mobile service provider.

• Don't reply to abusive or worrying text or video messages. Your mobile service provider will have a number for you to ring or text to report phone bullying. Visit their website for details.

• Don't delete messages from cyberbullies. You don't have to read them, but you should keep them as evidence.

Text harassment is a crime. If the calls are simply annoying, tell a teacher, parent or carer. If they are threatening or malicious and they persist, report them to the police, taking with you all the messages you've received.

Phone calls

If you get an abusive or silent phone call, don't hang up immediately. Instead, put the phone down and walk away for a few minutes. Then hang up or turn your phone off.

Once they realise they can't get you rattled, callers usually get bored and stop bothering you.

• Always tell someone else: a teacher, youth worker, parent, or carer. Get them to support you and monitor what's going on.

• Don't give out personal details such as your phone number to just anyone. And never leave your phone lying around. When you answer your phone, just say 'hello', not your name. If they ask you to confirm your phone number, ask what number they want and then tell them if they've got the right number or not. You can use your voicemail to vet your calls. A lot of mobiles display the caller's number. See if you recognise it. If you don't, let it divert to voicemail instead of answering it.

• And don't leave your name on your voicemail greeting. You could get an adult to record your greeting. Their voice might stop the caller ringing again.

Almost all calls nowadays can be traced.

If the problem continues, think about changing your phone number.

If you receive calls that scare or trouble you, make a note of the times and dates and report them to the police. If your mobile can record calls, take the recording too.

Emails

• Never reply to unpleasant or unwanted emails — the sender wants a response, so don't give them that satisfaction.

• Keep the emails as evidence. And tell an adult about them.

• Ask an adult to contact the sender's Internet Service Provider (ISP) by writing abuse@ and then the host, e.g. abuse@hotmail.com

• Never reply to someone you don't know, even if there's an option to 'unsubscribe'.

Replying simply confirms your email address as a real one.

Web bullying

If the bullying is on a website (e.g. Facebook) tell a teacher or parent, just as you would if the bullying was face-to-face – even if you don’t actually know the bully’s identity.

Serious bullying should be reported to the police - for example threats of a physical or sexual nature. Your parent or teacher will help you do this.

Chat rooms and instant messaging

• Never give out your name, address, phone number, school name or password online.

• It's a good idea to use a nickname. And don't give out photos of yourself.

• Don't accept emails or open files from people you don't know.

Remember it might not just be people your own age in a chat room.

• Stick to public areas in chat rooms and get out if you feel uncomfortable.

• Tell your parents or carers if you feel uncomfortable or worried about anything that happens in a chat room.

• Think carefully about what you write; don't leave yourself open to bullying.

• Don't ever give out passwords to your mobile or email account.

Three steps to stay out of harm's way

• Respect other people - online and off. Don't spread rumours about people or share their secrets, including their phone numbers and passwords.

• If someone insults you online or by phone, stay calm – and ignore them.

• Think how you would feel if you were bullied. You're responsible for your own behaviour – make sure you don't distress other people or cause them to be bullied by someone else

Appendix 6

Guidance on the Use of Communications Technologies

A wide range of communications technologies have the potential to enhance learning

• The official school email service is used for communications between staff, governors and with parents/carers and pupils, as it provides an effective audit trail.

• Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.

• Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.

• Pupils are taught about email safety issues through the scheme of work and implementation of the acceptable use policy.

• Personal information is not sent via e-mail as this is not secure. Personal information is also not posted on the school website

Appendix 9

Roles and Responsibilities

Governors

Approve and review the effectiveness of the E-Safety Policy and acceptable use policies

Ensure that the E-Safety Governor works with the ICT subject leader to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering and then reports to Governors

Have read, understood and signed the Staff, Governor and Visitor Acceptable Use Agreement (AUP)

Headteacher and Senior Leaders

Ensure that all staff receive suitable CPD to carry out their e-safety roles and sufficient resource is allocated.

Ensure that there is a system in place for monitoring e-safety

Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff

Inform the local authority about any serious e-safety issues including filtering

Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented.

ICT Leader

Deal with day to day e-safety issues

Lead role in establishing / reviewing e-safety policies / documents,

Ensure all staff are aware of the procedures outlined in policies

Provide and/or brokering training and advice for staff,

Attend updates and liaising with the Local Authority E-Safety staff and technical staff,

Deal with and log e-safety incidents including changes to filtering,

Report regularly to Senior Leadership Team

Teaching and Support Staff

Participate in any training and awareness raising sessions

Have read, understood and signed the Staff, Governor and Visitor Acceptable Use Agreement (AUP)

Act in accordance with the AUP and e-safety policy

Report any suspected misuse or problem to the E-Safety Co-ordinator

Monitor ICT activity in lessons, extra curricular and extended school activities

Students / Pupils

Participate in e-safety activities, follow the acceptable use policy and report any suspected misuse

Understand that the E-Safety Policy covers actions out of school that are related to their membership of the school

Parents and Carers

Endorse (by signature) the Student / Pupil Acceptable Use Policy

Ensure that their child / children follow acceptable use rules at home

Discuss e-safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet

Access the school website in accordance with the relevant school Acceptable Use Policy.

Keep up to date with issues through school updates and attendance at events

Technical Support

Ensure the school's ICT infrastructure is secure in accordance with Becta Provider guidelines and is not open to misuse or malicious attack

Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data

Inform the head teacher of issues relating to the filtering

Keep up to date with e-safety technical information and update others as relevant

Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction.

Ensure monitoring software / systems are implemented and updated

Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and that reasonable attempts are made to prevent spyware and malware.