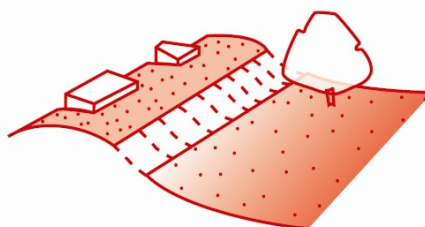


Riverhead Infants' School e-Safety Policy

Riverhead Infants' School



This policy was ratified by the Full Governing Body on

Heather

Signed

Chair of Governors

Heather Powell

Signed

Headteacher

Date:

11th May 2011

Next Review Date:

11th May 2014

Contents

- 1 e-Safety Policy Aims
 - 2.1 Teaching and Learning
 - 2.1.1 Why is Internet use important?
 - 2.1.2 How can Internet use enhance learning?
 - 2.1.3 How will pupils learn to evaluate content?
 - 2.2 Managing Internet Access
 - 2.2.1 How will information systems security be maintained?
 - 2.2.2 How will e-mail be managed?
 - 2.2.3 How will published content and the school website be managed?
 - 2.2.4 Can pupil images and work be published?
 - 2.2.5 How will social networking and personal publishing be managed?
 - 2.2.6 How will filtering be managed?
 - 2.2.7 How can emerging technologies be managed?
 - 2.2.8 How should personal data be protected?
 - 2.3 Policy Decisions
 - 2.3.1 How will Internet access be authorised?
 - 2.3.2 How will reported incidents be managed?
 - 2.3.3 How will risks be assessed?
 - 2.3.4 How will complaints be handled?
 - 2.4 Communications Policy
 - 2.4.1 How will the policy be introduced to the pupils?
 - 2.4.2 How will the policy be discussed with the Staff?
 - 2.4.3 How will parents' support be enlisted?
- 3 e-Safety Contacts and References
- 4 Legal Framework
- 5 Links to other policies
- 6 Appendices

1 e-Safety Policy Aims

It is the aim of the school to ensure safe access to the use of the Internet and digital communication technology ~~an~~ for all stakeholders within the school.

The e-Safety Policy is part of the suite of Safeguarding Policies. It has been written to enable the school to develop safe practice for all stakeholders and to ensure all are aware of their responsibilities in its implementation.

It is recognised that vulnerable pupils may be at greater risk in the use of the Internet and digital communication technology and for this reason all teaching staff are inducted in the implementation of this policy and the need for adaptation according to the individual needs of pupils.

To ensure effective implementation of this policy :

- The school will appoint an e-Safety Coordinator. This may be the Designated Child Protection Coordinator as the roles overlap.
- Our e-Safety Policy has been written building on the Kent e-Safety Policy and government guidance. It has been agreed by staff, senior management and approved by governors.
- The e-Safety Policy has had an Equality Impact Assessment completed.

2.2 Teaching and Learning

2.2.1 Why is Internet use important?

- 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 a part of the statutory curriculum and a necessary tool for staff and pupils.
- 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.

2.2.2 How can Internet use enhance learning?

- The school Internet access will be designed expressly for pupil use and includes 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.
- 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.

2.2.3 How will pupils learn how to evaluate Internet content?

- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law.

2.3 Managing Internet Access

2.3.1 How will information systems security be maintained?

- Staff will set their own passwords and they must be kept confidential.
- Users must take responsibility for their network use and ensure their use does not flout the Code of Conduct for ICT.
- Workstations should be secured against user mistakes and deliberate actions.
- School ICT systems capacity and security will be monitored regularly and reviewed annually.
- Virus protection will be updated daily and checked by the schools network manager during each visit.

Wide Area Network (WAN) security issues include:

- All Internet connections must be arranged via the KPSN Schools' Broadband Team to ensure compliance with the security policy.
- Central KPSN Schools Broadband firewalls and CPE's are configured to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership basis between schools and KCC/EIS.

The Schools Broadband network includes a cluster of high performance firewalls at each of the Internet connecting nodes. These appliances run industry leading software and are monitored and maintained by a specialist security command centre.

- The security of the school information systems and users will be reviewed regularly.
- Virus protection will be updated daily.
- Personal data sent over the Internet or taken off site will be encrypted.
- Files held on the school's network will be regularly checked.
- The network manager will review system capacity regularly.

2.3.2 How will e-mail be managed?

- Pupils may only use the approved e-mail software 2simple e-mail on the school system.
- The pupils will be taught how to use e-mail safely and effectively.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.

- With direct supervision of a teacher, e-mail may be sent or retrieved using a class e-mail address. The password for this will remain securely with the teacher and not revealed to the pupils.
- Staff will all be given e-mail accounts using web based Microsoft Outlook which is managed by the school technician. On leaving employment with the school the account will be stopped.
- All e-mails sent using the school e-mail system will include the school disclosure.
- E-mails will be monitored to ensure the e-mail system is being used appropriately and that the use of abusive language is not present.

2.3.3 How will published content and the school website be managed?

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.3.4 Can pupil's' images or work be published?

- The school does not allow children's full names to be published anywhere on the website,
- Photographs of pupils will not be accompanied by pupils' names.
- Written permission will be obtained from parents and carers before photographs of pupils are published on the website.

2.3.5 How will social networking and personal publishing be managed?

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

2.3.6 How will filtering be managed?

- The school will work with the KCC, BECTA and the Internet Service Provider to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the e-Safety Coordinator.
- Any material that the school believes is illegal must be reported to appropriate agencies such as the Internet Watch Foundation [IWF] or Child Exploitation and Online Protection Centre - [CEOP]

2.3.7 How can emerging technologies be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Pupils are not allowed to have mobile 'phones in school.
- Staff using smart-phones which access school e-mail will ensure effective passwords are used to protect data.

2.3.8 How should personal data be protected?

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

2.4 Policy Decisions

2.4.1 How will Internet access be authorised?

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the 'Staff Information Systems Code of Conduct' before using any school ICT resource.
- Children's access to the Internet will be under adult supervision to access specific, approved on-line materials.
- The Internet will only be used during lessons or adult led clubs and not at playtimes or lunchtimes.
- Parents will be asked to sign and return a consent form in their new entrants pack.

2.4.2 How will risks be assessed?

- 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 Kent can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.
- The Response to an Incident of Concern flow chart will be used to assess risk from an incident and the recommendation followed. Staff will seek advice from the Schools e-Safety Co-ordinator who is the school Designate Child Protection Co-ordinator.

2.4.3 Handling e-sSafety complaints

- Unacceptable use of the Internet or breach of the e-Safety Policy will be recorded using an e-Safety Record.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Complaints of Internet misuse will be dealt with by a senior member of staff, and, where necessary, the Complaints Policy will be applied.
- Any complaint about staff misuse must be referred to the Headteacher.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

2.4 Cyberbullying

- Cyberbullying, as with all forms of bullying, will not be tolerated.
- The school's Anti-Bullying Policy will be used to manage incidents of cyberbullying.
- Where incidents of cyberbullying occur out of school, the school will support pupils and parents/carers to manage the incident.

2.5 Effective communicating of this policy

2.5.1 How will the policy be introduced to pupils?

- e-Safety rules will be posted in all networked rooms and classrooms and discussed with the pupils at the start of each year.
- e-Safety strategies will be taught as part of the ICT Curriculum.
- Pupils will be informed that network and Internet use will be monitored.
- Useful e-Safety programmes include:
 - Think U Know: www.thinkuknow.co.uk
 - Childnet: www.childnet.com
 - www.kidsmart.org.uk
 - Safe Social Networking: www.safesocialnetworking.com

2.5.2 How will the policy be discussed with Staff?

- All staff will be given the school's e-Safety Policy, and its application and importance will be explained within induction procedures.
- e-Safety will form part of the suite of safeguarding policies and training will be provided within staff meetings for all members of staff.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential and expected.

2.5.3 How will parents' support be enlisted?

Parents' attention will be drawn to the school e-Safety Policy on the school website.

2.5.4 When will the policy be reviewed?

- The policy will be reviewed on an annual basis by the ICT Coordinator, the Headteacher, the school's ICT Technician and a member of the governing body
- The policy requires annual ratification by the Full Governing Body

3 e-Safety Contacts and References

Becta: www.becta.org.uk/safeguarding

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

CFE e-Safety Officer, KCC Children Families & Education

Rebecca Avery email: esafetyofficer@kent.gov.uk Tel: 01622 221469

Childline: www.childline.org.uk

Childnet: www.childnet.com

Children's Officer for Training & Development, Child Protection

Mike O'Connell email: mike.oconnell@kent.gov.uk Tel: 01622 696677

Children's Safeguards Service: www.kenttrustweb.org.uk/safeguards

Click Clever Click Safe Campaign: <http://clickcleverclicksafe.direct.gov.uk>

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

EIS - ICT Support for Schools and ICT Security Advice: www.eiskent.co.uk/ictsecurity

Internet Watch Foundation: www.iwf.org.uk

Kent e-Safety in Schools Guidance: www.kenttrustweb.org.uk/esafety (Includes a Schools Audit Tool and Notes on the Legal Framework as part of the PDF versions of this document)

Kent Primary Advisory e-Safety Pages: www.kenttrustweb.org.uk/kentict/kentict_home.cfm

Kent Public Service Network (KPSN): www.kpsn.net

Kent Safeguarding Children Board (KSCB): www.kscb.org.uk

Kidsmart: www.kidsmart.org.uk

Schools Broadband Team - Help with filtering and network security: www.eiskent.co.uk

Tel: 01622 206040

Schools e-Safety Blog: www.kenttrustweb.org.uk/esafetyblog

Teach Today: <http://en.teachtoday.eu>

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce – Report Abuse: www.virtualglobaltaskforce.com

4. Legal Framework

Notes on the legal framework

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 changes occur frequently. Please note this section is designed to inform users of legal issues relevant to the use of communications, it is not professional advice.

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.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003

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 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). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison.

The offence of grooming 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 etc fall into this category of trust).

Any sexual intercourse with a child under the age of 13 commits the offence of rape.

N.B. Schools should already have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

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)
- 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 (email) 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. This can include racist, xenophobic and homophobic comments, messages etc.

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 pertain (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 always advisable 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.

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 the 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.

This also includes incidents of racism, xenophobia and homophobia.

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.

Criminal Justice and Immigration Act 2008

Section 63 offence to possess "extreme pornographic image"

63 (6) must be "grossly offensive, disgusting or otherwise obscene"

63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic"

Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006

Education and Inspections Act 2006 outlines legal powers for schools which relate to cyberbullying/bullying:

Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.

School staff are able to confiscate items such as mobile 'phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy.

5 Links to other policies

- Child Protection Policy
- Whistle-blowing Policy
- Behaviour Policy
- Anti-Bullying Policy
- Single Equality Scheme
- Data Protection Policy
- Photographic Images Policy
- Special Educational Needs Policy
- Teaching and Learning Policy
- Schools ICT Security Policy

6 Appendices

- Schools and Setting E-Safety Policy Guidance
- Response to an Incident of Concern Flowchart
- e-Safety Classroom Poster
- e-Safety Report