Redhill Primary School

e -Safety Policy

Our Internet Policy has been written by members of our school Community, building on the Birmingham BGfL policy and government guidance. It has been agreed by the senior leadership team and approved by governors. It will be reviewed annually.

1   Use of the Internet at Redhill Primary School

Safe and responsible use of the Internet for the whole school community is at the heart of this policy.

2   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 management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in the 21st century for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience.

3 How does the Internet 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;
- access to experts in many fields for pupils and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the eg LA and DfES.

4 How will Internet use 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.

5 How will pupils learn to evaluate Internet content?

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Headteacher.

- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

6 How will e-mail be managed?

Pupils may only use approved e-mail accounts on the school system.

- Whole-class or group e-mail addresses should be used at Key Stage 2 and below.
- Access in school to external personal e-mail accounts may be blocked.
- Excessive social e-mail use can interfere with learning and will be restricted.
- E-mail sent to an external organisation 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
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils should never give out any information such as address or telephone number, or arrange to meet anyone.

7 How should Web site content be managed?

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs 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 Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- The Headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.
- Safeguarding procedures will be followed at all times.

8 What are newsgroups and e-mail lists?

- Newsgroups will not be made available to pupils unless an educational requirement for their use has been demonstrated.

9 Can Chat be made safe?

- Pupils will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will be supervised and the importance of chat room safety emphasised.

- A risk assessment will be carried out before pupils are allowed to use a new technology in school.

10 How can emerging Internet applications be managed?

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones should not be brought to school except in an emergency. They should be stored in the main office during the day and collected by pupils at home time. Their use in school is strictly forbidden.

11 How will Internet access be authorised?

- The school will keep a record of any pupils whose parents have specifically denied internet or e-mail access.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised Internet access (an example letter for primary schools is included as an appendix).
- Parents will be asked to sign and return a form stating that they have read and understood the Acceptable use document. Please see the sample form later in this document.
- Primary pupils will not automatically be issued with external individual email accounts, but will be authorised to us a group/class email address under supervision for external communication.

12 How will the risks be assessed?

- 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 BCC 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 policy is implemented and compliance with the policy monitored.
- All school computers will be monitored through the use of 'Policy Central' which will capture any material which may be deemed inappropriate and this can then be followed up.
- Safeguarding procedures will be followed at all times.

13 How will filtering be managed?

Despite careful design, filtering systems cannot be completely effective due to the speed of change of Web content. Filtering may be performed by the ISP, by the LA, at school-level or by any combination. School-level systems require considerable management to maintain effectiveness and place huge responsibility on the school if they are the only systems in place.

Careful monitoring and management of all filtering systems will be required. It is important that the school establishes the filtering criteria rather than simply accepting filtering default settings.

- The school will work in partnership with parents, the LA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.

If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to BCC using the e-mail filtering@bgfl.org via the Headteacher.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Policy Central will run regular reports to the Headteacher.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (please see references given later).

.

14 How will the policy be introduced to pupils?

- Rules for Internet access 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.
- Pupils will be reminded of the rules and risks at the beginning of any lesson using the Internet.

15 How will video conferencing be managed?

- All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- Equipment connected to the educational broadband network should use the national E.164 numbering system.
- External IP addresses should not be made available to other sites.
- Videoconferencing contact information will not be put on the school Website.
- The equipment must be secure and if necessary locked away when not in use.
- School videoconferencing equipment should not be taken off school premises without permission.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference. Recorded material shall be stored securely.

- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- If third party materials are to be included, checks will be made that recording is acceptable to avoid infringing the third party intellectual property rights.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate.

16 How will staff be consulted?

It is important that teachers and teaching assistants are confident to use the Internet in their work. The School E-Safety Policy will only be effective if all staff subscribe to its values and methods. Staff should be given opportunities to discuss the issues and develop appropriate teaching strategies. It would be unreasonable, for instance, if cover staff or supply staff were asked to take charge of an Internet activity without preparation. Clarification and discussion may be required.

- All staff is governed by the terms of the 'Responsible Internet Use' in school.
- All staff are aware of the use of 'Policy Central' on all computers in school and also on staff laptops.
- All staff including teachers, supply staff, classroom assistants and support staff, 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 operates monitoring procedures should be supervised by the Headteacher and report to them only.
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required.

17 How will ICT system security be maintained?

Local Area Network security issues include:

- The user must act reasonably. Loading non-approved software could cause major problems. Good password practice is required including logout after use.
- The workstation should be secure from casual mistakes by the user.
- Cabling should be secure and wireless LANs safe from interception.
- Servers must be located securely and physical access restricted.
- The server operating system must be secured to a high level.
- Virus protection for the whole network must be installed and current.

Wide Area Network (WAN) security issues include:

- All external connections must be assessed for security risks including the wide area network connection and any modems staff may wish to use.
- Firewalls and routers should be configured to prevent unauthorised use of software such as FTP and Telnet at the protocol level.

- Decisions on security made by external agencies such as the LEA or ISP must be discussed with schools. Third-party security testing should be considered.

- 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 LEA, particularly where a wide area network connection is being planned.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as floppy disks, memory sticks and CD-ROMs will be reviewed. Portable media may not be brought into school without specific permission and a virus check.
- 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 IT co-ordinator / network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

18. How will complaints regarding Internet use be handled?

- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about misuse must be referred to the Headteacher.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
- Sanctions available include:
  - interview/counselling by Headteacher or Deputy Headteacher ;

- informing parents or carers; denying access to the Internet
-

19 How will Cyberbullying be managed?

Cyberbullying can be defined as -

"The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007

Many young people and adults find using the internet and mobile phones a positive and creative part of their everyday life. Unfortunately, technologies can also being used negatively.

- Cyberbullying (as with all forms of bullying) will not be tolerated in school.
- All incidents of cyberbullying reported to the school will be recorded in the behaviour file.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where appropriate, such as examining system logs, identifying and interviewing possible witnesses, and

contacting the service provider and the police, if necessary.

Sanctions for those involved in Cyberbullying may include:

- The bully will be asked to remove any material deemed to be inappropriate or offensive.
- A service provider may be contacted to remove content.
- Internet access may be suspended at school for the user for a period of time.
- Parent/carers may be informed.
- The Police will be contacted if a criminal offence is suspected.

20. How will parents' support be enlisted?

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school Web site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

21. How is Internet used across the community?

- Example of Internet access rules in libraries:
- Adult users will need to sign the acceptable use policy.
- Parents/carers of children under 16 years of age will generally be required to sign an acceptable use policy on behalf of the child.

22. Newly emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Staff will be issued with a school phone where contact with pupils is required.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text, picture or video messages is forbidden.

23. Staff use of the Internet.

- Staff must adhere to all of the above when preparing lessons using the Internet.
- Personal use of the computer and Internet will also be permitted after 3.30pm and during a member of staff's lunch break and at no other time.
- Internet usage will be monitored on a regular basis.
- Staff using school laptops must also adhere to the Internet policy even when working out with the school premises.

24. How will e–Safety complaints be handled?

- Parents, teachers and pupils will be able to use the School's complaints procedure. The facts of the case will need to be established, for instance whether the Internet use was within or outside school.
- A minor transgression of the rules may be dealt with by a member of staff.
- Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. The anti – bullying policy will also be used as required.
- Potential child protection or illegal issues will always be referred to the school Designated Child Protection Person – the Headteacher or Deputy in her absence.
- Advice from the Police may be sought if there are suspicions of illegal practice.
- Any complaint about staff misuse must be referred to the Headteacher.
- All e–Safety complaints and incidents will be recorded by the school -including any actions taken – in the same way as bullying or racist incidents are recorded.
- Parents and pupils will be requested to work in partnership with staff to resolve issues.
- Any issues (including sanctions) will be dealt with according to the school's disciplinary and child protection procedures.

Failure to adhere to any of the above guidelines will result in the relevant disciplinary action being taken.

June 2014

Updated June 2016

Redhill Primary School

Responsible Internet Use

These rules help us to be fair to others and keep everyone safe.

- **I will ask permission before using the Internet.**
- **I will use only my own network login and password, which is secret.**
- **I will only look at or delete my own files.**
- **I understand that I must not bring software or disks into school without permission.**
- **I will only e-mail people I know, or my teacher has approved.**
- **The messages I send will be polite and sensible.**
- **I understand that I must never give my home address or phone number, or arrange to meet someone.**
- **I will ask for permission before opening an e-mail or an e-mail attachment sent by someone I do not know.**
- **I will not use Internet chat.**
- **I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher immediately.**
- **I understand that the school may check my computer files and the Internet sites I visit.**
- **I understand that if I deliberately break these rules, I may not be allowed to use the Internet or computers.**

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of ICT skills, Redhill Primary School is providing supervised access to the Internet. We believe that the effective use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Responsible Internet Use and sign and return the consent form so that your child may use Internet at school.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use (or to see a lesson in operation) please telephone me to arrange an appointment.

Yours sincerely

J Jones
Headteacher

Redhill School Responsible Internet Use Agreement.

Redhill School

Responsible Internet Use

Please complete, sign and return to the school secretary

Pupil: ***Form:***

Pupil's Agreement

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.

Signed: ***Date:***

Parent's Agreement for Internet Access

I have read and understood the school rules for responsible Internet use. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the ICT facilities.

Signed: ***Date:***

Please print name:

Parent's Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter's work may be published on the school Web site. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.

Signed: ***Date:***

This consent form is based, with permission, on the Internet Policy of the Irish National Centre for Technology in Education.

References

Particularly for Parents and Children

National Action for Children (NCH) www.nchafc.org.uk/itok/
Parents Guide on Internet usage

Bullying Online www.bullying.co.uk
Advice for children, parents and schools

FKBKO - For Kids By Kids Online www.fkbko.co.uk
Excellent Internet savvy for kids; KS1 to KS3

Parents Information Network (PIN) www.pin.org.uk
Comprehensive guidelines on Internet safety

Parents Online www.parentsonline.gov.uk/2003/parents/safety/index.html
Interactive learning and safety advice, excellent presentation for parents.

Kidsmart www.kidsmart.org.uk
An Internet safety site from Childnet, with low-cost leaflets for parents.

Think U Know? www.thinkuknow.co.uk/
Home Office site for pupils and parents explaining Internet dangers and how to stay in control.

Family Guide Book (DfES recommended www.familyguidebook.com
Information for parents, teachers and pupils

NCH Action for Children www.nchafc.org.uk
Expert advice for children, young people and parents.

Safekids www.safekids.com
Family guide to making Internet safe, fun and productive

Particularly for Schools

Associations of Co-ordinators of IT (ACITT)
Acceptable use policy for the Internet in UK Schools, original straightforward text.
www.g2fl.greenwich.gov.uk/acitt/resources/assoc/aup97.doc

NAACE / BCS www.naace.org (publications section)
A guide for schools prepared by the BCS Schools Committee
and the National Association of Advisers for Computer Education (NAACE)

DfES Superhighway Safety http://safety.ngfl.gov.uk
Essential reading, both Web site and free information pack. Telephone: 0845 6022260

KS2 Internet Proficiency Scheme
www.becta.org.uk/corporate/corporate.cfm?section=8&id=2758
A Becta, DFES and QCA pack to help teachers educate children on staying safe on the internet

Internet Watch Foundation - www.iwf.org.uk
Invites users to report illegal Web sites

Data Protection www.informationcommissioner.gov.uk/
New Web site from the Information Commissioner

Kent Web Skills Project www.kented.org.uk/ngfl/webskills/
Discussion of the research process and how the Web is best used in projects.

Click Thinking: Scottish Education Department www.scotland.go
Comprehensive safety advice

Kent ICT Security Policy www.kent.gov.uk/eis (broadband link)
An overview of the need to secure networks with Internet access.

Copyright www.templetons.com/brad/copymyths.html
Irreverent but useful coverage of the main aspects of copyright of digital materials, US-based.

Internet Users Guide www.terena.nl/library/gnrt/
A guide to network resource tools, a book (ISBN 0-201-61905-9) or free on the Web.

Alan November – The Grammar of the Internet www.edrenplanne
Article explaining how to evaluate Web sites and information

DotSafe – European Internet Safety Project http://dotsafe.
A comprehensive site with a wide range of ideas and resources, some based on Kent work.

Cybercafe http://www.gridclub.com/home_page/hot_headlines/cyber.shtml
Internet proficiency through online games for KS2, with a free teacher's pack.

Acknowledgements

We wish to thank many people including teachers and officers from Kent, members of SEGfL, NAACE and the British Computer Society Expert Schools Panel.

John Allen, School Effectiveness; Steve Bacon, NAACE; Clive Bonner, EIS; Ian Coulson, School Effectiveness; Sandra Crapper, Consultant; Kevin Figg, Westlands; Maureen

Gillham, Weald of Kent Grammar; Michael Headley, EIS; Greg Hill, SEGfL; Andrew Lamb, Whitfield Primary; Paul Newton, Kent NGfL; Richard Packham, EIS; Ian Price, Child Protection; Sandra Patrick, Kent NGfL; Tom Phillips, KCC; Graham Read, Simon Langton Girls Grammar; Martin Smith, Highsted Grammar; Chris Shaw, EIS; Linda Shaw, Kent NGfL; Chris Smith, Hong Kong; John Smith, Wakefield LEA; Helen Smith, Kent NGfL; Laurie Thomas, KCC; Clare Usher, Hugh Christie; Gita Vyas, Northfleet School for Girls; Carol Webb, Cornwallis; Ted Wilcox, Borden Grammar. Roger Blamire, BECTa; Stephanie Brivio, Libraries; Les Craggs, KAS; Alastair Fielden, Valence School; John Fulton, Hartsdown; Keith Gillett, Seal Primary; Doreen Hunter, Deanwood Primary Technology School; Steve Murphy, Drapers Mills Primary; Judy Revell, KCC; Chris Ridgeway, Invicta Grammar; Nick Roberts, Sussex LEA; Graham Stabbs, St Margarets at Cliffe Primary; Sharon Sperling, KCC; Brian Tayler, KCC; Joanna Wainwright, KCC; Richard Ward, KCC; Theresa Warford, Libraries; Ian Whyte, Plaxtol Primary; Chris Woodley, KCC.

Notes on the legal framework

This page must not be taken as advice on legal issues, but we feel that schools should be alerted to some of the legislation that may be relevant.

The Computer Misuse Act 1990 makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998. The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day to day activities.

A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interests of amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.

Schools could start by banning private use of a school's computer system, but then allow private use following application to the head teacher. The Rules for Responsible Internet Use, which every user must agree to, contain a paragraph that should ensure users are aware that the school is monitoring Internet use.

In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring.

The following legislation is also relevant:

Data Protection Act 1984/98 concerns date on individual people held on computer files and its use and protection.

Copyright, Design and Patents Act 1988 makes it an offence to use unlicensed software

The Telecommunications Act 1984 Section 43 makes it an offence to send offensive or indecent materials over the public telecommunications system.

Protection of Children Act 1978

Obscene Publications Act 1959 and 1964 defines “obscene” and related offences.

References:

Brief introduction to dangers and legal aspects of the Internet.
www.bbc.co.uk/webwise/basics/user_01.shtml

List of useful law resources; see copyright and Internet sections.
http://link.bubl.ac.uk/law

HMSO: Full text of all UK legislation and purchase of paper copies.
www.legislation.hmso.gov.uk