Alkrington Primary School

E-Safety Policy

1. Introduction

The Internet is now regarded as an essential resource to support teaching and learning. The statutory curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning, such as phones and touch screen tablet devices. Computer skills are vital to access life-long learning and employment; indeed ICT is now seen as an essential life-skill. Young people have access to the Internet from many places, home, school, friends' homes, libraries and in many cases mobile phones. Schools have a number of services to help ensure that curriculum use is safe and appropriate, however, access out of school does not usually have these services and has a range of risks associated with its use. Schools are ideally placed to help young people learn to become e-safe. This policy is designed to ensure safe internet use by pupils in school, but also while on-line at home etc.

2. Core Principles of Internet Safety

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies such as mobile phones.
There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

3. Why is Internet use important?

• 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.
• The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, well-being and to support the professional work of staff and to enhance the school's management information and business administration systems.

4. How will Internet use enhance learning?

• The school Internet access will be designed expressly for educational use and will include filtering appropriate to the age of pupils.
• Pupils will learn appropriate Internet use and be given clear objectives for Internet use.
• 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 Internet access be authorised?

• The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date; for instance a member of staff may leave or a pupil's access be withdrawn.
• Primary pupils will not be issued individual email accounts, but will be authorised to us a group/class email address under supervision.
• There is a structured approach to internet access and internet searches, with clear progression through the school. This can be seen in the Computing planning overview.

6. How will filtering be managed?

• The school will work in partnership with parents; Rochdale Council, and EDIT to ensure systems to protect pupils are

reviewed and improved.
• If staff or pupils discover unsuitable or illegal sites, the URL (address) and content must be reported to the ICT co-ordinator or any responsible adults.
Parents of the children involved will be notified.
• Website logs will be regularly sampled and monitored.
• The ICT technician, working alongside the Computing co-ordinator will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

7. 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 Rochdale Council 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 and Computing Co-ordinator will ensure that the Internet policy is implemented and compliance with the policy monitored.

8. Managing Content

8.1 How will pupils learn to evaluate Internet content?
• Schools should ensure that staff and pupils are aware that the use of internet derived materials should comply with current copyright laws.
• Specific lessons will be included within the Computing Scheme of Work that teaches all pupils how to read for information from web resources.
• Nominated persons (Computing technician) will be responsible for permitting and denying additional websites as requested by colleagues.

8.2 How should website content be managed?
• The point of contact on the website should be the school address, school e-mail and telephone number. The named contact will be the schools' Business Manager. Staff or pupils' home information will not be published.
• Website photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name.
• Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website, and where pupils are on the child protection register, information may only be added at the discretion of the Safeguarding lead.

9. Communication

9.1 Managing e-mail and online communication formats (OCF)
• Pupils may only use approved e-mail and OCF accounts on the school system.
• Pupils must immediately tell a teacher if they receive offensive e-mail or messages.
• Pupils must not reveal details of themselves or others in communications, such as address or telephone number, or arrange to meet anyone.
• Whole-class or group e-mail and OCF addresses should be used.
• E-mail and OCF messages 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.

9.2 On-line communications and social networking.
• Pupils will be taught about how to keep personal information safe when using online services. Each year group will have specific Computing lessons dedicated to e-safety.
• The school will conduct annual pupil surveys about home use of ICT. It will gauge the range of activities which pupils undertake and how safely they are using them, e.g. keeping personal information safe, experiences of cyber bullying etc.

• The use of online chat is not permitted in school, other than as part of its online learning environment.

9.3 Mobile technologies
• Appropriate use of mobile phones will be taught to pupils as part of their e-safety programme.
• Pupil mobile phones are not permitted within the school.
• Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

10. Introducing the Policy to Pupils

• Rules for Internet access will be displayed within school.
• A module on responsible Internet use and e-safety will be included in the curriculum covering both school and home use. This will include the necessity of keeping personal information safe, how to use mobile technologies appropriately and using online communication appropriately.
• Instruction on responsible and safe use should precede Internet access.
• Pupils will be informed that Internet use will be monitored.
• All Key Stage 1 &2 pupils will use the e-safety activities from the Alkrington Primary Schools Computing Scheme of Work to help teach Internet Safety.

11. Parents and E-Safety

• Parents' attention will be drawn to the School E-Safety Policy in newsletters and on the school Website.
• Regular information will be provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home. This will be done through regular e-safety workshops for parents.
• 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.
• All parents will receive support information as and when available.

12. Consulting with Staff and their inclusion in the E-safety Policy

• All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the Internet Access Statement, and its importance explained.
• The school's consequences for Internet and mobile phone / PDA / technology misuse will be clear so that all teachers are confident to apply this should the situation arise.
• All staff must accept the terms of the 'Acceptable Use' statement before using any Internet resource in school.
• Staff should be aware that Internet traffic is monitored and reported by the EDIT and can be traced to the individual user. Discretion and professional conduct is essential.
• Community users of the school's ICT facilities must sign the acceptable use policy before being granted access.
• The school will adopt the Council's e-mail and Internet user policy.
• The monitoring of Internet use is a sensitive matter. Staff that operate monitoring procedures should be supervised by senior management.
• Staff development in safe and responsible Internet use and on the school Internet policy will be provided as required, but not less than once a year.

13. How will complaints be handled?

• Responsibility for handling incidents will be delegated to a senior member of staff.
• Any complaint about staff misuse must be referred to the Headteacher.
• Parents and pupils will need to work in partnership with staff to resolve issues.
• There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Review Date: Sept 2018

Appendices

Alkrington Primary School
Rules for 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 class or own network login and password.
• I will only open or delete my own files.
• I understand that I must not bring into school and use software or files without permission.
• I will only e-mail and open attachments from 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.
• If 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, e-mails I send 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.]

Laptop policy for Alkrington Primary School staff

1. The laptop remains the property of Alkrington Primary School.
2. The laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Alkrington School Staff should use the laptop.
3. On the teacher leaving the school's employment, the laptop is returned to Alkrington Primary School.
Staff on extended leave of 4 weeks and over should return their laptops to the school (other than by prior agreement with the Headteacher).
4. When in school and not being used, the laptop must be kept secured in the Computing suite, locked room or office. It must not be left in an unlocked, unattended classroom.
5. Whenever a laptop is taken out of school, it is the responsibility to ensure that the laptop is secured in line with insurance policy coverage, which is the responsibility of the individual to maintain.
6. The laptop must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the Headteacher with evidence of adequate insurance.
7. Staff may load their own software onto the laptop but it must be fully licensed and not corrupt any software or systems already installed on the laptop.
8. Any software loaded must not affect the integrity of the school network.
9. If any removable media is used then it must be checked to ensure it is free from any viruses.
10. It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop is kept up-to-date.
11. Staff must use their laptop in school on the network at least once a week to ensure virus protection is automatically updated.
12. Staff should not attempt to significantly alter the computer settings other than to personalise their desktop working area.
13. If any fault occurs with the laptop, it should be referred immediately to the Computing technician, via the log book.

Web-based Resources
For Schools

KidSmart http://www.kidsmart.org.uk/
SMART rules from Childnet International and Know It All for Parents
Childnet International http://www.childnet-int.org/
Guidance for parents, schools and pupils
Becta http://schools.becta.org.uk/index.php?section=ise-Safety Advice
Becta / Grid Club, Internet Proficiency Scheme
On-line activities for Key Stage 2 pupils to teach e-safety.
http://www.gridclub.com/teachers/t_internet_safety.html
DfES Anti-Bullying Advice http://www.dfes.gov.uk/bullying/
Grid Club http://www.gridclub.com/teachers/t_internet_safety.html
Internet Watch Foundation www.iwf.org.uk
Invites users to report illegal Websites
South West Grid for Learning – Safe www.swgfl.org.uk/safe
Think U Know www.thinkuknow.co.uk/

For Parents

https://www.saferinternet.org.uk/advice-centre/parents-and-carers
www.childnet.com/blog/free-internet-safety-leaflets-for-parents-2016
https://www.thinkuknow.co.uk/parents/
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/

Kids Smart http://www.kidsmart.org.uk/parents/advice.aspx
A downloadable PowerPoint presentation for parents
Childnet International http://www.childnet-int.org/
“Know It All” CD-ROM free to order resource for parents to help raise awareness of how to help their children stay safe online.