Acklam Whin Primary School

E– Safety & Acceptable Use Policy

Reviewed: September 2016

E-Safety Policy –

Introduction

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and electronic publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to make safe and responsible decisions in order to control their online experience.

At Acklam Whin, we understand the importance of effective e-safety practice for both staff and pupils and the e-safety policy sets out how we ensure this is achieved.

The school's e-safety policy operates in conjunction with other policies including those for Behaviour, Anti-Bullying, Curriculum policies and Data Protection.

E-Safety in school

E-Safety depends on effective practice at a number of levels:

- Responsible use of technologies by all staff, pupils and governors; encouraged by the curriculum and made explicit through published policies.
- Sound implementation of the e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering systems.

1.0 School e-safety policy

1.1 Writing and reviewing the e-safety policy

The e-Safety Policy relates to other policies including those for ICT and for child protection.

- The school has appointed an e-Safety Coordinator who is also the schools Safeguarding officer. She works in close co-operation with the headteacher.
- Our e-Safety Policy has been written by the school. It has been agreed by the staff and governors.
- E-Safety issues are included in the Child Protection, Data Protection, Health and Safety, Anti-Bullying, PSHE and Computing policies.
- The e-Safety Policy will be reviewed in June 2017

1.2 Teaching and learning

1.2.1 Why Internet use is 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.
- Internet use is a part of the curriculum and a necessary tool for staff and pupils.

1.2.3 Internet use will enhance learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils.
- Pupils will be taught what Internet use is acceptable and what is not, and will be given clear objectives for Internet use, using the SMART rules (See Appendix 2).
- Internet access will be planned to enrich and extend learning activities.
- Staff will guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

1.2.4 Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the school e-Safety Coordinator.
- Staff should ensure that the use of Internet derived materials by staff and by 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.

1.3 Managing Internet Access

1.3.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses broadband with an effective firewall and filters.

1.3.2 E-mail

- Pupils may only use approved e-mail accounts, via the VLE, on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- 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.
- 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.

1.3.3 Published content and the school web site

- The contact details on the Web site 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.

1.3.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' 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 Twitter or Facebook.
- Pupil's work can only be published with the permission of the pupil and parents.

1.3.5 Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are taught never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc. (See Appendix 2 - The SMART Rules).
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils as many have age restrictions (See Appendix 5).

1.3.6 Managing filtering

- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school E-Safety coordinator.
- Senior staff will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

1.3.7 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones will not be used by pupils at Acklam whin Primary . The sending of abusive or inappropriate text messages on the way to and from school is forbidden and will be reported to parents and the headteacher.
- Staff will not contact pupils using email or phone (mobile or land line). Parents will not be contacted by mobile phone unless urgent contact is required and for school business, e.g. an emergency with their child on a school trip.

1.3.8 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The school is registered with the Information Commission Ofice and will adhere to the legal requirement for use and storage of personal/sensitive data.
- All access to personal data will be password protected.

1.4 Policy Decisions

1.4.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff, including Teaching Assistants and Supply Teachers must read and sign the ICT Acceptable User Policy (AUP) before using any school ICT resource (See Appendix 4).
- At FSƒKey Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents and pupils will be asked to sign and return a consent form agreeing to comply with the school's Acceptable Use Policy (See Appendix 3).

1.4.2 Assessing risks

- 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. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- The headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

1.4.3 Handling e-safety complaints

- Complaints of Internet misuse involving the pupils will be dealt with by a senior member of staff. Sanctions resulting may include interviewƒcounselling by class teacher ƒ headteacher; informing parents or carers; removal of Internet or computer access for a period of time.
- Any complaint about staff misuse must be referred to the head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

1.4.4 Community use of the Internet

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

1.5 Communications Policy

1.5.1 Introducing the e-safety policy to pupils

- Rules for Internet access will be posted in all networked rooms (See Appendix 5).
- Pupils will be informed that Internet use will be monitored.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use (See Appendix 2).

1.5.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff should be aware that Internet trafic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

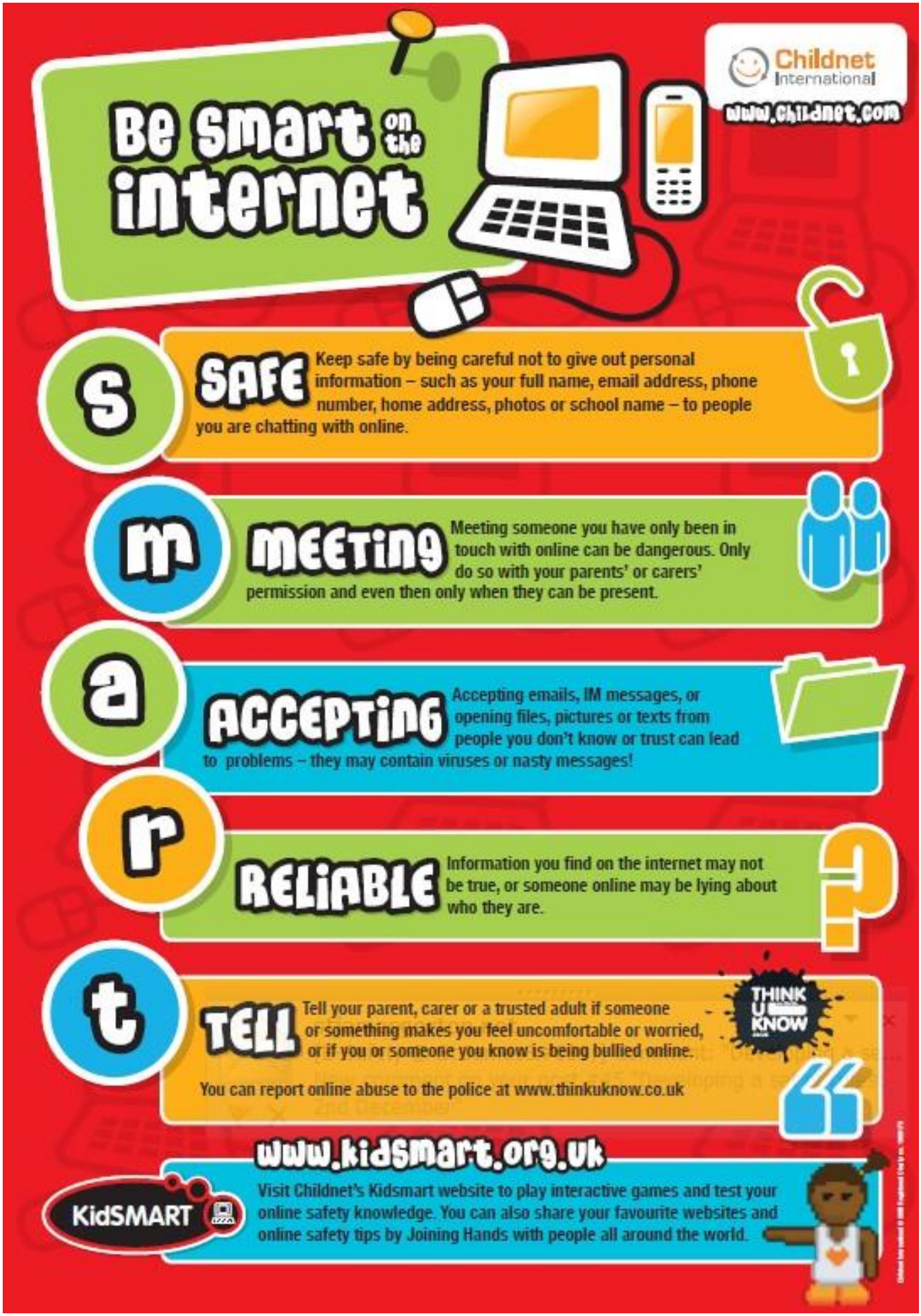
1.5.3 Enlisting parents'/carers' support

- Parents' ƒ carers' attention will be drawn to the School e-Safety Policy in newsletters and on the website.
- A school document 'A Parents' Guide to Video Games and Online Safety' will be issued to all new parents in school and be accessible through the school website (See Appendix 6).
- School, through the headteacher or Deputy headteacher, will contact parents where concerns have been raised about a pupil's access to age-inappropriate games, DVDs etc.

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key e-safety issues	Relevant websites
Creating web directories to provide easy access to suitable	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	
Using search engines to access information from a range of websites.	Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.	Safe Search for Kids Ask Jeeves for kids CBBC Search
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information.	VLE Email GridClub E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted.	School website VLE
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name.	School website VLE
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	VLE GridClub
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	VLE

Appendix 2: Internet use - The SMART Rules



Appendix 4:

Acklam Whin Primary
Staff and Governor
Technology Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with Jodie Short or Darren Gamble.

- I will only use the school's hardware ƒ email ƒ Internet ƒ Learning PlaVorm 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 are compatible with my professional role.
- I will not contact pupils using email or phone (mobile or land line). Parents will not be contacted by personal mobile phone unless urgent contact is required and for school business, e.g. an emergency with their child on a school trip.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory, and will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- Images of pupils and or staff will only be taken, stored and used for professional purposes in line with school policy and with the consent of the parent/carer. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff or Headteacher.
- 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, to the Headteacher. I will respect copyright and intellectual property rights.
- I will support and promote the school's e-Safety (including data security) policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.

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

Full Name
…….....(printed)

Appendix 5: Internet use - Rules for Responsible Internet Access

Acklam Whin

Rules for Responsible Use of Technology

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

☐ I will only use school computers for schoolwork.

☐ I will only use the internet when my teacher has given me permission.

☐ I will always be polite when using the internet, VLE or email.

☐ I will not download files or bring in disks or USB memory sticks from outside the school unless I have been given permission.

☐ I will NEVER give out my address or telephone number to any other internet user.

☐ I will only send email that my teacher has approved so that they can be sure I am kept safe.

☐ If I am uncomfortable or upset by anything I discover on the internet, I will report it to an adult immediately.

☐ I will only use search engines that my teacher has approved.

☐ I understand that if I fail to keep these rules, I will not be allowed to use the internet in school.

SeUng up parental controls.

Besides checking PEGI ratings to help choose suitable games, parents can activate parental controls. This is much easier than it sounds and links to instructions can be found on our school website ‘Parents’ pages for many of the latest generation of game consoles - including Xbox 360, Wii U™, Sony Playstation 3 and PSP, Apple and PC controls.

Using these controls, you can restrict the rating or level of content that your child can play, and in some cases who your child plays with online and for how much time.

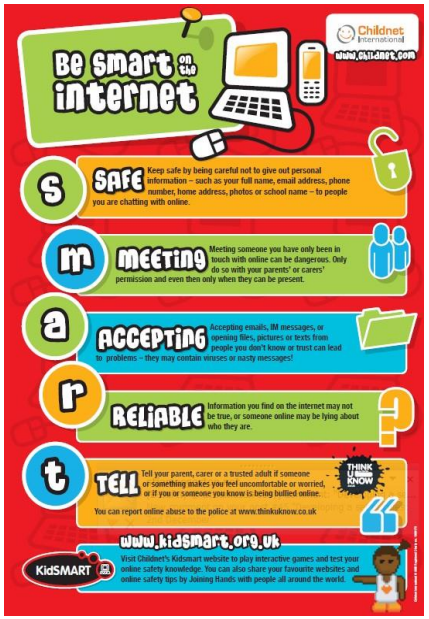
Parental controls ensure that your child has a fun and secure gaming experience.

Making sure your child’s video game experience is safe and secure.

At Acklam whin, we ensure that the children know how to keep themselves safe online and what to do if they feel uncomfortable about any content they might see.

The children also learn how to behave responsibly online both at home and at school in order to make everyone’s online and gaming experience a good one.

We follow the SMART rules, which can be found on our school website.



Acklam Whin School

A Parent’s Guide to Video

A guide for parents about choosing age appropriate games, setting up parental controls, and making sure your child's video game experience is safe and secure.

Video games are a great source of learning and entertainment, but it is important for parents to appreciate what playing games today involves in order to keep their children safe.

A large number of games can be played over an internet connection. Being aware of the tools at a parent's disposal are crucial to ensure that children are safeguarded from inappropriate content and encounters with other players.

Some widely available video games contain graphic violence, virtual sex, violent and gory scenes, partial or full nudity, drug use, portrayal of criminal behaviour or other provocative and sensitive material.

Online gaming platforms often offer text chat, the use of headsets or even video for live communication with other players. Unfortunately, the anonymity of online gaming seems to encourage some players to post obscenities and unsuitable material which are dificult to control.

A Parents' and Carers' Guide to Video Game Ratings

It is probably true that most parents have grown up with the video or DVD classification system. However, this is not always the case with video games. All too often, the child is more adept at using the computer or games consoles and parents do not know how to access what he or she is playing. As a result, it is important to have something to guide parents when making a decision about whether a game is suitable or not.

The PEGI System (Pan-European Game Information)

From the summer of 2012, the PEGI system has been used by UK law for age rating video games. The age ratings 12, 16 and 18 are mandatory and it is illegal for a retailer to supply any game to someone below the age specified.

It is important to note that the age ratings relate to the content of the game and not how dificult it is to play. So, for example, a chess game would be too dificult to give to a 3 year old but it will have a '3' rating as the content is inoffensive. Likewise, a game which is easy enough for a 10 year old to play will be given an '18' rating if the subject matter or content is only suitable for adults. Therefore, a '3' or '7' rating does not mean that the game will be too easy for your child but that the content is suitable for primary age children.

Descriptors shown on the back of the packaging indicate the main reasons why a game has received a particular age rating. There are eight descriptors: violence, bad language, fear, drugs, sexual, discrimination, gambling and online gameplay with other people.

Further information on the PEGI ratings can be found at : http:ffwww.pegi.infofenfindexfidf33f