



Kereseforth Primary School

E-Safety Policy

CONTENTS

1. Why is the internet important?	Page 3
2. How will internet use enhance learning?	Page 3
3. How will pupils learn to evaluate internet content?	Page 4
4. How should website content be managed?	Page 5
5. Can social media/text messaging be made safe?	Page 6
6. Log-on to the computer and internet.	Page 6
7. How will the risks be assessed?	Page 7
8. How will complaints regarding internet use be handled?	Page 7
9. Who is responsible for e-safety?	Page 8
10. Acceptable use policies.	Page 8
11. Appendices	Page 9

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. Computer skills are vital to access life-long learning and employment. Computing is now seen as an essential life-skill.

Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which – as in life generally – may be unsuitable. It is important that schools, libraries and youth clubs, as well as parents adopt strategies for the safe and responsible use of the Internet.

Our E-safety Policy has been written by the Computing Coordinator using Barnsley Learning Network and government guidance. It has been agreed by senior management and governors. It will be reviewed biannually.

Why is internet use important?

The internet is an essential element in 21st century life for education, business and social interaction. As a school, we have a duty to provide students with quality internet access as part of their learning experiences.

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 learn appropriate internet use, what is and what is not appropriate use, and given clear objectives for internet use.

Staff should guide pupils in online 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. They will be taught a range of skills including researching, for example knowledge location, retrieval and evaluation as well as skills such as uploading work and images to share with other learners.

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;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- 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 LA and DSCF.

How will pupils learn to evaluate internet content?

The quality of information received via the range of media is variable and everyone needs to develop skills in selection and evaluation. The spreading of malicious rumour has occurred for thousands of years and lies sometimes win over truth. Information received via the web, e-mail or text message also requires good information handling skills. In particular, it may be difficult to determine origin and accuracy, as the contextual clues present with books or TV may be missing or difficult to read.

It is a sad fact that pupils may occasionally be confronted with inappropriate material, despite all attempts at filtering. Pupils should be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example: to close the page and report to a trusted adult. Children should also be taught what to do if they experience this sort of material outside the safety of school, as e-safety is a skill all children will require for the future. Children should be shown how and where to report unreasonable actions and materials, for example at the websites, www.thinkuknow.co.uk or www.ceop.gov.uk.

More often, pupils will be judging reasonable material but need to select that which is relevant to their needs, for instance to answer a particular question. Pupils should be taught research techniques and encouraged to question the validity, currency and origins of information. Effective guided use should also reduce the opportunity pupils have for exploring undesirable areas.

Using Internet derived materials in pupils' own work requires at least an understanding that straight copying is worth little without a commentary that demonstrates the selectivity used and evaluates significance. Pupils should be

taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

How should website content be managed?

Many schools have created excellent web sites that inspire pupils to publish work of a high standard. Web sites can celebrate pupils' work, promote the school and publish resources for projects or homework. Editorial guidance will ensure that the Web site reflects the school's ethos that information is accurate and well-presented and that personal security is not compromised. Although there are many ways to obtain information about schools and pupils, for instance a school newsletter, a school's web site can be accessed by anyone on the Internet. Publication of information should be considered from a security viewpoint.

Photographs that include pupils add a liveliness and interest to a web site that is difficult to achieve in any other way. Nevertheless, the security of staff and pupils must come first. Sadly, although common in newspapers, the publishing of pupils' names with photographs of pupils is not acceptable. Web images could be misused and individual pupils identified unless broad descriptions are used. The following point should be adhered to:

- a) A check should be made that pupils in photographs are appropriately clothed.
- b) 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.
- c) Web site photographs that include pupils will be selected carefully and pupils' full names will not be used anywhere on the web site, particularly in association with photographs.
- d) Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site. A parent consent form is signed at enrolment at school.
- e) The class teacher will have the responsibility of checking that all children seen on photographs uploaded to the shared drive for the website have parental permission for their photographs to be online.

Can Social Media/Text Messaging be made safe?

Messenger is a popular conferencing application offering instantaneous exchange of text and images between groups of users via the Internet. In principle, messenger has great potential for education; for instance, pupils could exchange live text, speech or video with pupils in South Africa or Italy, at low cost. Such chat facilities should be moderated by the parents/guardians and access should only be at times permitted by the parent/guardian.

Although many social media apps are not allowed in Keresforth Primary School and are not legally allowed to be accessed until age 13, their use by pupils outside school is becoming more common. The approach therefore that parents and teachers need to take is one of keeping aware of developments and advising their children of the dangers. Information for parents about current apps that staff are aware of is shared with parents on the school X page. Children need to ensure that they protect their social media account with a password (which needs to be constantly updated) and report any incidents concerning inappropriate or graphic messages or images. Alongside this, children should make their social media account 'private' so that no one, other than people they choose to allow, can see their posts/images/personal details. They also need to be made aware that sharing inappropriate messages or images is very serious and would be dealt with accordingly. This information will be shared with children, but it is up to parents to monitor. Parents looking to find resources on how to keep their children safe online can go to the parent's section on our school website to find several e-safety resources (<https://www.keresforthprimary.org.uk/e-safety/>).

Children should not bring any mobile phone into school. If they are walking to and from school and therefore carry a mobile with them, it must be handed in at the office before the start of the day and collected after school.

Log-On to the Computer and Internet

To encourage independence and personal responsibility children must be taught to log-on independently, it is a valuable life skill. To avoid or reduce any potential problems all IT users should abide by the following

- a) All of Key Stage 2 should allow time for the children to develop these skills they should be incorporated into the teachers' planning during the first term of each new academic year.

- b) Under no circumstances should the teacher use their own personal log-in (even as well-meaning as it might be) to log the child onto the computer/system.
- c) If a child has forgotten their log-in the teacher can speak to the IT technician in school and retrieve it. This normally takes only a couple of days.
- d) A child will have to share a computer with a friend until this matter has been resolved.
- e) KS1 provision to be made to assist the child to log-on, but again not to use the teacher's/assistant's profile.

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. Children will be taught how to best deal with this situation.

How will complaints regarding internet use be handled?

Teachers must report any incidents they come across (whether that is themselves, or been told by parents/children) on CPOMS tagging the DSL team. Prompt action will be required if a complaint is made. 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 the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to the school's behaviour policy. Complaints of a child protection nature must be dealt with in accordance with the LA child protection procedures.

- a) Responsibility for handling incidents regarding child protection will be delegated to the DSL team.
- b) Any complaint about staff misuse must be referred to the head teacher.
- c) Parents and pupils will need to work in partnership with staff to resolve issues.

- d) There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

Who is responsible for e-safety?

- Children
- Parents and guardians
- Teachers and other school staff
- School's computing coordinator
- DSL team
- Head teacher
- Governors

Everyone who uses electronic devices is responsible for e-safety. Children should be taught at school and at home how to use the internet in a safe and responsible manner, as well as what to do if they see something that they are not comfortable with.

Acceptable Use Policies

There are two acceptable use policies, a KS1 and a KS2. The rules within each policy help us to be fair to others and keep everyone safe online. Children sign the appropriate policy as they enter each Key Stage. The rules should be recapped at the start of every school year and more regularly if the teacher deems it to be necessary.

See appendices for KS1 (appendix 1a) and KS2 (appendix 1b) acceptable use policies.

Created by: Miss Pearson – Computing Coordinator
Date: April 2020

Reviewed by: Miss Ogle – Computing Coordinator
Date: November 2024

Appendices

Appendix 1a

Acceptable Use Policy - Key Stage 1

I will follow these rules to keep me safe

- I will not damage any school-owned ICT equipment.
- I will not eat or drink while using school-owned ICT equipment.
- I will make sure I take care of any school-owned ICT equipment that I use in school.
- I will only use the internet when my teacher says I can.
- I will listen carefully to all the teachers and follow their instructions.
- I will only use the school's computers for my school work.
- I will only log on as myself.
- I will turn off the monitor if I see something that I feel uncomfortable with or upsets me; then I will tell my teacher straight away.
- I will not have my own email address.
- I will only be able to use the class email when I am working with my teacher.
- I know that some websites and social networks have age restrictions and I should not use them unless I am old enough.
- I will not say nasty or hurtful things about any member of staff or pupil online.
- I will not try and get to any websites that the school has blocked access to.
- I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my safety.
- I will never arrange to meet anyone I have only met online.

Name _____

Signed: _____

Date: _____

Appendix 1b

Acceptable Use Policy - Key Stage 2

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements

- I have read and know what the computer rules in this document mean to me.
- I will only go on the internet using my own username and password.
- I will make sure that my password for the internet is difficult to guess and I will not share my password with anybody else.
- If I think someone has guessed my password, I will tell a teacher.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I see anything like this, I will tell my teacher immediately.
- I will not try and get to any websites that the school has blocked access to.
- I will make sure I take care of any school-owned ICT equipment that I use in school.
- I will not install any software on school computers.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my safety.
- I will not damage any school-owned ICT equipment.
- I will not eat or drink while using school-owned ICT equipment.

Social Media

- I know that some websites and social networks have age restrictions and I should not use them unless I am old enough.
- I will not say nasty or hurtful things about any member of staff or pupil online.

- I will not give away any of my personal details (full name, age, date of birth, sex, address etc.) or the personal details of other users in school, over the internet. This includes photographs or video images of me, other pupils or members of staff.
- I will never arrange to meet anyone I have only met online unless a trusted adult is with me.
- If I see any hurtful comments about the school, staff or pupils. I will take screenshots for evidence and report to the e-Safety coordinator in school.

Managing Digital Content

- I will only use school-owned equipment to create pictures, video and sound. Pictures, video and sound will not be taken without asking permission first.
- I will not publish anything online, e.g. images or pictures, without asking my teacher.

Mobile phones and devices

- I will not bring my mobile phone or other devices to school without permission from my teacher.
- If I do need to bring my mobile phone to school, it will be kept at the school office until home time.
- I will not use or take pictures in school on my mobile phone or mobile device.

Name: _____

Signed: _____ Date: _____