Royles Brook Primary School Policy on e-Safety

(see also Computing Policy)

Teaching and Learning

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 statutory curriculum and a necessary tool for staff and pupils.

Internet use will 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. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate Internet content

The school will ensure that the use of Internet derived materials by staff and pupils comply 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.

Managing Internet Access

Information system security

School computing systems capacity and security will be reviewed regularly. Virus protection will be updated regularly. Once a week, an update of children's usage on the school laptops is sent, via email, to both the Headteacher and the subject leader.

E-mail

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

Published content and the school web site

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.

Publishing pupil's images and work

Photographs that include pupils will be selected carefully. Pupils' full names will not be used anywhere on the Website in association with photographs. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website or Learning Platform (public area). Pupil's work can only be published with the permission of the pupil and parents.

Social networking and personal publishing

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.

Managing filtering

The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved. If pupils or staff discover an unsuitable site, it must be reported to the Class Teacher, eSafety Officer or Head Teacher. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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. The use of portable media such as memory sticks will be monitored closely as potential sources of computer virus and inappropriate material. Pupils should not normally bring mobile phones to school. When this is absolutely necessary, pupils' mobile phones will be kept in the school office and returned to pupils at the end of the school day. The sending of abusive or inappropriate text messages is forbidden. Staff will use a school phone where contact with pupils is required.

Protecting personal data

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

Policy Decisions

Authorising Internet access

Pupil instruction in responsible and safe use should precede any Internet access and all pupils must sign up to the Pupil eSafety Agreement to abide by the school's eSafety Rules. These eSafety Rules will also be displayed clearly in all networked rooms. Access to the Internet will be by directly supervised access to specific, approved on-line materials. All parents will be asked to sign the Parent eSafety Agreement giving consent for their child to use the Internet in school by following the school's eSafety Rules and within the constraints detailed in the school's eSafety Policy. All staff must read and agree in writing to adhere to the Acceptable Use of the Internet Agreement for Staff before using any school computing web-based resource.

Assessing risks

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 the Local Authority can accept liability for the material accessed, or any consequences of Internet access. The school will audit computing provision to establish if the eSafety Policy is adequate and that its implementation is effective.

Handling eSafety complaints

Complaints of Internet misuse will be dealt with by a senior member of staff. 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. Pupils and parents will be informed of the complaints procedure.

Community use of the Internet

External organisations using the school's computing facilities must adhere to the eSafety Policy.

Communications Policy

Introducing the eSafety Policy to pupils

eSafety rules will be posted in all networked rooms and discussed with the pupils at the start of each year. Pupils will be informed that network and Internet use will be monitored**.**

Staff and the eSafety Policy

All staff will be given the School eSafety Policy and its importance explained. Any information downloaded must be respectful of copyright, property rights and privacy. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software.

Enlisting parents' support

Parents' attention will be drawn to the School eSafety Policy in newsletters and on the School Website.

Monitoring and review

This policy is implemented on a day-to-day basis by all school staff and is monitored by the Computing Leader. This policy is the Governors' responsibility and they review its effectiveness annually. They do this during reviews conducted between the eSafety Leader, Computing Leader, Designated Child Protection Coordinator, Governor with responsibility for Computing and Governor

with responsibility for Child Protection. Ongoing incidents would be reported to the full governing body.

Written by Mr C Morris – April 2018

Date for review: Spring 2020

Appendix 1: Internet use – Possible teaching and learning activities

Activities Key eSafety issues Relevant websites

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.

Web quests e.g. Ask Jeeves for kids

Yahooligans

CBBC Search

Kidsclick

Exchanging information with other pupils and asking questions of experts via e-mail.

Pupils should use only approved email accounts.

Pupils should never give out personal information.

Consider using systems that provide online moderation

e.g. Grid Club

ePals

Super Clubs PLUS

email a children's author

email Museums and Galleries

Making the News

Super Clubs

Infomapper

Headline History

Focus on Film

Making the News

Super Clubs

Learning grids

Museum sites, etc.

Digital Storytelling

BBC – Primary Art

Audio and video

conferencing to

gather information

and share pupils'

work.

Skype

Flash Meeting

National Archives "On-Line"

Global Leap

National History

Museum

Imperial War Museum

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.

Pupils should be supervised. Only sites that are secure and need to be accessed using an email address or protected password should be used.

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.