E-SAFETY POLICY

Body Responsible for the Policy	Full Governing Body (FGB)
Date Policy endorsed by the FGB	December 2017
Date of Next Review	October 2019
Name of Headteacher	Mrs Lesley Spicer

1. References

- Anti Bullying Policy
- Child Protection Policy
- Computing Policy

2. Introduction

Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials. Parents will be asked to sign and return a consent form.

Writing and reviewing the e-safety policy

- The designated e-Safety Coordinator is Sylma Gordon who has child protection training. It is not a technical role.
- Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.
- The e-Safety Policy was revised by Sylma Gordon.

3. Teaching and Learning

3.1 Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school aims 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.

3.2 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering provided by Hampshire County Council to its schools.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.

3.3 Pupils will be taught how to evaluate Internet content

- The school will acknowledge the source of Internet derived materials by staff and pupils e.g. photographs when necessary.
- When evaluating Web content, pupils will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening. For example, to tell the teacher who will decide if the URL* needs to be included in the list of blocked sites by Hampshire County Council. If this is the case, the teacher will report the incident to the e-safety co-ordinator manager who will have the site blocked.

* This is the Uniform Resource Locator (URL). A URL can be thought of as the "address" of a web page and is sometimes referred to informally as a "web address."

4. Managing Internet Access	

4.1 Information system security

- Virus protection will be updated regularly by Hampshire County Council.
- Security strategies are provided by Hampshire County Council.

4.2 Email

- Pupils may only use approved e-mail accounts on the school system.
- Pupils are encouraged to immediately tell a teacher if they receive offensive emails.
- In email communication, pupils will be taught not to reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming email should be treated as suspicious and attachments not opened unless the author is known.
- No anonymous email or chain email will be forwarded.

4.3 Published content and the school web site

- Staff or pupil personal contact information will not be published on the school website. The contact details given online is the school office details.
- As many authorised users can update the school website, the author and date of publication will be identified in the administrator's section.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

4.4 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully so that individual pupils cannot be identified, or their image misused. Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site or other on-line space.
- Pupils full names will not be used anywhere on the school web site or other on-line space, particularly in association with photographs.
- Work can only be published with the permission of the pupil and parents/carers.

4.5 Social networking and personal publishing

- Newsgroups* will not be used.
- Pupils will be advised never to give out personal details of any kind which may identify them or their friends.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and secret code words when using social networking sites.

* (an open discussion group devoted to a selected topic. When you post to a newsgroup anyone is able to see your message and respond)

4.6 Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator who will inform Hampshire County Council of the URL for inclusion in their list of blocked sites.

4.7 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.
- The appropriate use of Learning Platforms continues to be discussed as the technology becomes more widely used within the school.
- Staff will not take images of children on mobile phones.

4.8 Protecting personal data

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

4.9 Monitoring

The school complies with HCC's Email and Internet Monitoring Policy. This states that:

The County Council reserves the right to monitor the use of email, Internet and Intranet communications and where necessary data may be accessed or intercepted in the following circumstances:

- To ensure that the security of the County Council's computer hardware, software, networks or systems are not compromised;
- To prevent or detect crime or unauthorised use of the County Councils computer hardware, software, networks or systems;
- To gain access to communications where necessary when a user is absent from work.

Staff who have internet access during the course of their work should be made aware that the school/County Council may track the history of the internet sites they have visited.
The County Council respects the right of individuals to privacy of communications. At the same time it has a duty to protect the interests of itself and others against unlawful use of its computer facilities. To balance these needs, interception of personal and private communications will not normally take place unless grounds exist to show evidence of some crime or other unlawful or unauthorised use.

Access to personal and private communications will normally only take place with the approval of the Director of Human Resources, or designated representative, in conjunction with the Head of IT

Services and Headteacher/Chair of Governors or with the approval of the Chief Internal Auditor and/or Monitoring Officer. Such access will only be authorised following an assessment to determine what, if any, access or interception is justified.

5. Policy Decisions

5.1 Authorising Internet access

- All staff must read and sign the "Staff Code of Conduct for ICT" before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- Any person not directly employed by the school will be asked to sign an "acceptable use of school ICT resources" before being allowed to access the internet from school hardware.

5.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor HCC can accept liability for any material accessed, or any consequences of Internet access.

5.3 Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the head teacher.
- 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 (see schools complaints policy).
- Pupils who break the school's internet rules will be dealt with according to the severity of the breach. As an infant school we acknowledge that this is unlikely to occur. However, for most first offences the pupil would have to explain the school's internet rules to the class teacher and it will again be emphasised how important it is for these to be followed. Parents would be contacted and asked to reiterate the importance of following the school's e-mail and internet rules. Any further breaches could result in the withdrawal of logon rights and pupils would only be able to practise ICT through a much restricted access (direct supervision by an adult*).*
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

6. Communications Policy

6.1 Introducing the e-safety policy to pupils

- E-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- A programme of training in e-Safety is followed based on the materials from Child Exploitation and Online Protection centre (CEOP) using the think you know website.
- E-Safety training will be embedded within the ICT scheme of work and the Personal Social and Health Education (PSHE) curriculum.

6.2 Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff are informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff will always use a child friendly safe search engine when accessing the web with pupils. (see appendix 1)

6.3 Enlisting parents' and carers' support

- Parents/carers attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.

7. 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 websites.	Parental consent should be sought. Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Webquest UK Kent Learning Zone The School Website
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. 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.	CBBC Search Kidsclick
Exchanging information with other pupils and asking questions of experts via e-mail or blogs.	Pupils should only use approved e-mail accounts or blogs. Pupils should never give out personal information. Consider using systems that provide online moderation e.g. SuperClubs Plus.	RM EasyMail SuperClubs Plus School Net Global Kids Safe Mail
Publishing pupils' work on school and other websites.	Pupil and parental consent will be sought when children join the school. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on moderated sites.	School website Espresso National Education Network Gallery BBC – Primary Art Learninggrids Museum sites, etc.
Publishing images including photographs of pupils.	Parental consent for publication of photographs will be sought when children join the school. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.	Making the News School Website
Audio and video conferencing to gather information and share pupils' work	Pupils should be supervised. Schools should only use applications that are managed by Local Authorities and approved Educational Suppliers.	National Archives "On-Line" JANET Videoconferencing Advisory Service (JVCS)

8. Appendix 2

Useful Resources for Teachers

BBC Stay Safe
www.bbc.co.uk/cbbc/help/safesurfing/

Chat Danger
www.chatdanger.com

Child Exploitation and Online Protection Centre
www.ceop.gov.uk/

Childnet
www.childnet-int.org/ (provides links to other sites mentioned here)

Digizen
www.digizen.org/

Kidsmart
www.kidsmart.org.uk/ (under 11 area junior orientated)

Think U Know
www.thinkuknow.co.uk/ (5-7 section) - Hectors World and new characters Lee and Kim.

9. Appendix 3

Useful Resources for Parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf
(Internet safety Tips for parents)

Family Online Safe Institute
www.fosi.org