Bevendean Primary School

eSafety Policy & Acceptable Use Policy

This policy was adopted in **January 2015**

This Policy is due for review in **January 2019**

CONTENTS

1.0 Introduction

The policy outlines purposes and guidelines in provision of email facilities, use of digital equipment and internet access to both and staff. The e-Safety Policy is part of the ICT Policy and should relate to other policies including those for ICT, Bullying, Child Protection, Behaviour, PSHE and citizenship.

The e-Safety Policy has been written by the school, building on government guidance. It has been agreed by the senior management and approved by governors.

The e-Safety Policy and its implementation will be reviewed annually by the Senior Management Team, the ICT coordinator, ICT technician and network manager.

2.0 Teaching and learning

2.1 Why the Internet and digital communications are important

- The purpose of Internet use, digital communication and digital equipment in school is to raise educational standards, promote pupil achievement, to support the professional work of staff and to enhance school's management functions.
- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.2 Using the Internet to 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.
- Internet access will be planned to enrich and extend learning activities.

2.3 Teaching pupils how to evaluate Internet content

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils in Key Stage 2 should be taught the importance of cross-checking materials and information from various sources and how to validate information before accepting its accuracy.
- Pupils will be taught to report unpleasant internet content. Reminders of this are in 'Our Internet Safety Code' (*Appendix 5*) which is displayed in every pupil workstation

2.4 Making Internet Access Safe

- Children using the Internet will be working in the classroom or ICT suite under adult supervision.
- Pupils will not be allowed access to the Internet during wet lunch or playtimes unless supervised by their class teacher.
- Staff will check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils.
- Staff will be particularly vigilant when pupils are undertaking their own searches.
- Pupils will be taught to use e-mail and the Internet responsibly in order to reduce the risk to themselves and others.
- Our Internet Safety Code is posted near all pupil access workstations (*Appendix 5*).
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from the LA, our Internet Service Provider and the Department for Children Schools and Families (DCSF).
- Pupils are taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

2.5 Expectations

- Pupils are expected to play their part in reducing the risk of viewing inappropriate material by following our Internet Safety Code and school rules with regards to any anti-social or bullying behaviour.
- If pupils abuse the privileges of access to the internet or use of e-mail facilities by failing to follow the rules they have been taught then sanctions consistent with our School Behaviour Policy. Pupils may be given reduced access to the Internet. This also applies with regards to any misuse of any type of electronic messaging method either inside or outside school which constitutes bullying or other anti-social behaviour.

3.0 Managing Information Systems

3.1 Information systems security

- The security of the school information systems will be reviewed regularly.
- Virus protection is installed for the whole network and will be updated regularly.
- Security strategies will be discussed with Brighton and Hove ICT support team.
- The network manager will review system capacity regularly.
- Servers are located securely and physical access restricted.
- The server operating system is secured and kept up to date.
- Only school purchased and licensed software will be loaded onto the network and computers.
- Access by wireless devices must be individually approved.
- Personal data sent over the internet will be encrypted or otherwise stored securely (*working towards*).
- Portable media may not be used without specific permission.

- Good password practice is required including logout after use.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached emails.
- Files held the school's network will be regularly checked.
- The ICT co-coordinator / network manager / ICT technician will review system capacity regularly.
- Data access is only given to appropriate users. (*see Data Security Policy*)

3.2 Managing Email

- Pupils may only use approved email accounts (Yr1 upwards).
- Every step is taken to minimize the risk of children being exposed to spam and junk mail.
- Teachers should review pupil's emails regularly.
- Pupils must immediately tell a teacher if they receive offensive email.
- Pupils must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission.
- Pupils will be taught to treat incoming emails from unknown senders as suspicious and not to open attachments from such emails.
- All emails from the school, especially those to external bodies, should be appropriate. The teacher is responsible for checking that this is the case.
- Whole-class or group email addresses are currently used. It is not proposed at present to give out individual email accounts. This will remain under review.
- Staff must use their local authority email (iMail) account for all emails relating to school matters. Staff personal email addresses should not be accessed by pupils or parents. Any email sent between staff and parents/carers should be sent through their school iMail account and the Head teacher should be copied in.
- Access in school to personal email accounts may be blocked.

3.3 Published content and the school website

- Information published on the website should be accurate and up to date.
- The contact details on the website are for the school address, email and telephone number. Staff or pupils personal information must not be published.
- Responsibility for what appears on Year group pages lies with the class teachers.
- The website managers: ICT coordinator, Network manager, Business manager and head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

3.4 Publishing pupils' images and work

- Images that include pupils will be selected carefully and will not enable individual pupils to be clearly identified. We will always consider using group photos rather than individuals.
- 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 images of pupils are electronically published.
- The website should comply with the local authority guidelines for publications.
- Work can only be published with permission of the pupil and parent *(Appendix 4*) and copyright material will be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

3.5 Social networking and personal publishing

- The schools will block/filter access to social networking sites via Brighton and Hove firewall.
- 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 and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended and email addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name or school.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers will be advised not to run social network spaces for student use on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Schools should be aware that bullying can take place through social networking and gaming networks especially when a space has been setup without a password and others are invited to see the bully's comments.

3.6 Managing filtering

- The school will work with Local Authority (LA) to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL(web address) must be reported to the e-Safety Coordinator.

3.7 Managing videoconferencing/use of webcams

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the pupils' age.
- *These are guidelines as this technology in not currently used.*

3.8 Managing online chat rooms social networks

- Pupils and staff are not allowed to access public or unregulated websites.
- Children will use only regulated educational chat environments. This use will always be supervised and the importance of chat room safety emphasised.
- The school does not allow access to any social networking sites such as Facebook or Beebo.

3.9 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. This will be carried out by senior staff, in collaboration with the LEA.
- All staff should be aware that Bluetooth devices and mobile internet access can bypass the school's filtering system.
- Mobile phones are not allowed in school for most pupils. Currently, year 6 may bring in a phone but hand it in at the office for the day. The sending of abusive or inappropriate text messages is forbidden and will be assessed according to the school's bullying policy.

3.10 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. (*Appendix 3*)
- Personal data should be kept secure.

4.0 Policy Decisions

4.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the Staff Information Systems Code of Conduct before using any school ICT resource. Any person not directly employed by the school will be asked to sign the acceptable use policy before being allowed to use ICT resources.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form for pupil access.
- Parents will be informed that pupils will be provided with supervised Internet access.

4.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use, but will work to limit any problems that arise.

- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission of for inappropriate purpose could constitute a criminal offence under the Computer Misuse Act 1990. (*Appendix 2*)

4.3 E-safety complaints procedure

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy include:
  - interview by the head of year.
  - informing parents or carer.
  - removal of Internet or computer access for a period.

4.4 Community use of the internet

- Bevendean Primary school is a community school, made available to outside organizations out of school hours. These organizations are responsible for their users and use of the internet.
- The school will be sensitive to Internet related issues experienced outside by pupils outside of school, e.g. social networking sites, and offer appropriate advice.

4.5 Introducing the policy to pupils

- E-Safety rules will be posted in rooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- E-safety module will be included in the PSHE, Citizenship or ICT schemes of work covering both school and home use.

4.6 Introducing the policy to staff

- All staff will be given the School e-Safety Policy and its application and importance explained. (*Appendix 6*)
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.

4.7 Enlisting the support of parents

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, the school brochure and on the school website. (*Appendix 3*)
- The school will ask all parents to sign the parent/pupil agreement in the acceptable use policy. (*Appendix 4*)

- The attached list of e-safety resources may be of use to parents as well as teachers. (*Appendix 1*)

4.8 Internet Incidents

- Responsibility for handling incidents involving children will be taken by the ICT Co-ordinator and the Headteacher and the pupil's class teacher.
- If appropriate, teaching staff will be made aware of the incident and children involved.
- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support.
- The pupil's parents/carers will be informed of the incident and the course of action the school has taken.
- If staff or pupils discover unsuitable sites, the ICT co-ordinator will be informed. They will report the URL (web address) and content to the Internet Service Provider (ISP) and the Local Authority (LA). If it is thought that the material is illegal, after consultation with the ISP and LA, the site will be referred to the Internet Watch Foundation and the police.

5.0 APPENDIX 1

e-Safety Resources

BBC Chat Guide

http://www.bbc.co.uk/chatguide/

Becta

http://www.becta.org.uk/schools/esafety

Childline

http://www.childline.org.uk/

Child Exploitation & Online Protection Centre

http://www.ceop.gov.uk

e-Safety in Schools

http://www.kenttrustweb.org.uk?esafety

Grid Club and the Cyber Cafe

http://www.gridclub.com

Internet Watch Foundation

http://www.iwf.org.uk/

Internet Safety Zone

http://www.internetsafetyzone.com/

Kent Primary Advisory e-Safety Pages

http://www.kented.org.uk/ngfl/ict/safety.htm

http://www.kenttrustweb.org.uk/kcn/e-safety_home.cfm

Kidsmart

http://www.kidsmart.org.uk/

NCH – The Children's Charity

http://www.nch.org.uk/information/index.php?i=209

NSPCC

http://www.nspcc.org.uk/html/home/needadvice/needadvice.htm

Schools e-Safety Blog

http://clusterweb.org.uk?esafetyblog

Schools ICT Security Policy

http://www.eiskent.co.uk (broadband link)

Stop Text Bully

www.stoptextbully.com

Think U Know website

http://www.thinkuknow.co.uk/

Virtual Global Taskforce – Report Abuse

http://www.virtualglobaltaskforce.com/

6.0 APPENDIX 2

Notes on the legal framework

This section is designed to inform users of legal issues relevant to the use of electronic communications. It is not professional advice. Many young people and indeed some staff use the Internet regularly without being aware that some of the activities they take part in are potentially illegal. The law is developing rapidly and recent changes have been enacted through:

¤ • The Sexual Offences Act 2003, which introduces new offences of grooming, and, in relation to making/distributing indecent images of children, raised the age of the a child to 18 years old;

¤ • The Racial and Religious Hatred Act 2006 which creates new offences involving stirring up hatred against persons on religious grounds; and

¤ • The Police and Justice Act 2006 which extended the reach of the Computer Misuse Act 1990 making denial of service attacks a criminal offence.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape. N.B. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

More information about the 2003 Act can be found at www.teachernet.gov.uk

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Children, Families and Education Directorate page 37 April 2007

Data Protection Act 1998

The Act requires anyone who handles personal information to notify the Information Commissioner‟s Office of the type of processing it administers, and must comply with important data protection principles when treating personal data relating to any living individual. The Act also grants individuals rights of access to their personal data, compensation and prevention of processing.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual‟s motivation, the Act makes it a criminal offence to:

¤ • gain access to computer files or software without permission (for example using someone else‟s password to access files);

¤ • gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or

¤ • impair the operation of a computer or program (for example caused by viruses or denial of service attacks).

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author‟s own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. It is an infringement of copyright to copy all or a substantial part of anyone‟s work without obtaining the author‟s permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else‟s material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Children, Families and Education Directorate page 38 April 2007

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

7.0 APPENDIX 3

Bevendean Primary School – Internet Use Policy
Information for Parents

The Internet is an essential element in 21st century life. The school has a duty to provide students with quality Internet access as part of their learning.
Pupils often use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

- School Internet access is designed for pupil use and includes security filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not.
- Pupils will be taught to report unpleasant internet content.

Email

Whole-class or group email addresses are currently used. It is not proposed at present to give out individual email accounts. This will remain under review. Pupils will be taught to write friendly and polite emails, to treat unknown senders as suspicious and to report offensive material.

The school website

The school website is secure as only users who log in with a password can access pupils' pages. It is a safe way for children to explore blogs and forums as well as to access work set for them by their teacher. We will keep the security of this site under review.

- Pupils should keep their login details secret and use a strong password.
- Website use is monitored by teachers.
- Pupils full names will not be used anywhere on the website, particularly in association with photographs.
- We will ask your permission to use photographs of your child. Where possible we will use group photos rather than individual ones.

Social networking and personal publishing

- The School does not allow access to social networking sites. However, your child will be taught about responsible and safe use of these sites as more and more children are using them at home.
- Staff will not accept pupils at the school as friends on their social networking sites but will communicate with their class through the school website, which can be monitored.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use, but will work to limit any problems that arise.

E-safety complaints procedure

- Complaints of Internet misuse will be dealt with by a senior member of staff and e-safety coordinator.
- Please refer any complaint about staff misuse to the Head teacher.
- Parents and pupils will need to work in partnership with staff to resolve issues.
- Sanctions within the school discipline policy include:
    - ✓ Interview by a senior member of staff
    - ✓ informing parents or carers;
    - ✓ removal of Internet or computer access for a period.

Please fill in and return the attached consent form. If you would like any further information about Internet safety please contact the school office.

8.0 APPENDIX 4

Bevendean Primary School

e-Safety Rules

All pupils use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-Safety Rules have been understood and agreed.

Pupil:	***Class:***

Pupil's Agreement

- I have read and I understand the school e-Safety Rules.
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times.
- I know that network and Internet access may be monitored.

Signed:	***Date:***

Parent's Consent for Web Publication of Work and Photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the school rule that photographs will not be accompanied by pupil names.

Signed: ***Date:***

Parent's Consent for Internet Access

I have read and understood the school e-safety rules and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the school cannot be held responsible for the content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed:	***Date:***

Please print name:

Please complete, sign and return to the school office.

9.0 APPENDIX 5

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails together.

We can write polite and friendly emails to people that we know.

Think then Click

e-Safety Rules for Key Stage 2

- We ask permission before using the Internet.
- We only use websites that an adult has chosen or approved.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only email people an adult has approved.
- We send emails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not open emails sent by anyone we don't know.
- We do not use Internet chat rooms.

10.0 APPENDIX 6

Staff Code of Conduct for ICT

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's e-safety policy for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras; email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems may not be used for private purposes without specific permission from the headteacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not install any software or hardware without discussion with the ICT coordinator and ICT technician.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the e-Safety Coordinator, the Designated Child Protection Coordinator or Headteacher.
- I will ensure that electronic communications with pupils including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept email and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and accept the Staff Code of Conduct for ICT.

Signed: …… Capitals: …… Date: ……

Accepted for school: …… Capitals: ……