



E-Safety Policy 2017

Policy Contact Person	Mr Charlie Lindsay
Next Review Date	January 2018
Review Frequency	Annually
Governor's Signature	
Date Signed	
Signed original stored in Business Manager's Office	



1. Introduction

Our E-Safety Policy has been written by the school with contributions from staff and pupils. It has been agreed by the Senior Leadership Team and approved by Governors. The Policy will be reviewed annually. The Head acts as the E-Safety Co-ordinator.

2. Background and Rationale

2.1 The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even truer for children and young people, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that children and young people learn and are taught. At home, technology is changing the way children and young people live and the activities in which they choose to partake; these trends are set to continue.

2.2 While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- a. Access to illegal, harmful or inappropriate images or other content.
- b. Allowing or seeking unauthorised access to personal information.
- c. Allowing or seeking unauthorised access to private data, including financial data.
- d. The risk of being subject to grooming by those with whom they make contact on the internet.
- e. The sharing / distribution of personal images without an individual's consent or knowledge.
- f. Inappropriate communication / contact with others, including sexting and stranger danger.
- g. Cyber-bullying.
- h. Access to unsuitable video / internet games.
- i. An inability to evaluate the quality, accuracy and relevance of information on the internet.
- j. Plagiarism and copyright infringement.
- k. Illegal downloading of music or video files.
- l. The potential for excessive or addictive use which may impact on social and emotional development and learning.
- m. The potential to be drawn into terrorism through radicalisation via social media.

2.3 This policy sets out how we strive to keep pupils safe with technology while they are in school. We recognise that children and young people are often more at risk when using technology at home (where often no controls over the technical structures are put in place to keep them safe) and so this policy also sets out how we educate them about the potential risks and try to embed appropriate behaviours. We also explain how we attempt to inform those people who work with our pupils beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

3. Why is Internet use important?

3.1 The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems.

3.2 Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access.

3.3 Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

4. How does Internet use benefit education?

Benefits of using the Internet in education include:

- a. access to world-wide educational resources including museums and art galleries;
- b. educational and cultural exchanges between pupils world-wide;
- c. access to experts in many fields for pupils and staff;
- d. professional development for staff through access to national developments, educational materials and effective curriculum practice;
- e. collaboration across support services and professional associations;
- f. improved access to technical support including remote management of networks and automatic system updates;
- g. exchange of curriculum and administration data with the Local Authority and the Department for Children, Schools and Families (DCSF); access to learning wherever and whenever convenient.

5. How can Internet use enhance learning?

- a. The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- b. Pupils will be taught the types of Internet use that are acceptable and not acceptable and will be given clear objectives for Internet use.
- c. Internet access will be planned to enrich and extend learning activities.
- d. Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- e. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

6. Authorised Internet Access

- a. The school will maintain a current record of all staff and pupils who are granted Internet access.
- b. All staff must read and sign the 'Acceptable Computing Use Agreement' before using any school computing resource.
- c. Parents will be informed that pupils will be provided with supervised Internet access.
- d. Parents will be asked to sign and return a consent form for pupil access.
- e. Pupils will also be asked to sign an Acceptable Use Agreement. There is a simpler form for most of the school and a more comprehensive form for years 5 & 6. Examples of both forms are shown in Appendix 2.

7. World Wide Web

- a. If staff or pupils discover unsuitable sites, the URL (address), time, content must be logged and reported to the Local Authority helpdesk via the E-safety Co-ordinator or Network Manager.
- b. The school will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- c. Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

8. Email

- a. Pupils may only use approved e-mail accounts on the school system.
- b. Pupils must immediately tell a teacher if they receive offensive e-mail.
- c. Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- d. Access in school to external personal e-mail accounts may be blocked.
- e. E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- f. The forwarding of chain letters is not permitted.

9. Social Networking

- a. Our school blocks/filters access to social networking sites and newsgroups unless a specific use is approved.
- b. Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- c. Pupils will be advised not to place personal photos on any social network space.
- d. Pupils will be advised on security and encouraged to set strong passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others.

10. Filtering

The school will work in partnership with the Local Authority, and the Internet Service Provider to ensure filtering systems are as effective as possible.

11. Video Conferencing

- a. Video conferencing should use the educational broadband network rather than the Internet to ensure quality of service and security.
- b. Pupils must ask permission from the supervising teacher before making or answering a video conference call.
- c. Video conferencing will be supervised appropriately according to the pupils' age.

12. 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.

13. Mobile Phones

Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden. Pupils' mobile phones are to be left at the school office.

14. Information System Security

School Computing systems, capacity and security will be reviewed regularly. Virus protection will be installed and updated regularly. Security strategies will be discussed with the Local Authority.

15. Protecting Personal Data

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

16. Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor East Sussex County Council can accept liability for the material accessed, or any consequences of Internet access. The school will monitor Computing use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate.

17. Handling E-safety Complaints

- a. Complaints of Internet misuse will be dealt with by a senior member of staff.
- b. Any complaint about staff misuse must be referred to the Headteacher.
- c. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- d. Pupils and parents will be informed of the complaints procedure.
- e. Discussions will be held with the Police Community Support Officer (PCSO) with regard to the handling of potentially illegal issues.

18. Handling of E-safety incidents

A simple flow chart is displayed in all classrooms and the Computing suite showing the children what they should do if they encounter a problem. A more detailed flow chart for staff actions is also displayed in all classrooms and the Computing suite. Copies of both flow charts are included in Appendix 4.

19. Communication of Policy

Rules for Internet access will be posted in all networked rooms. Pupils will be informed that Internet use will be monitored. All staff will be shown the School E-Safety Policy and its importance explained. Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential. Parents' attention will be drawn to the School E-Safety Policy in newsletters, the school prospectus and on the School Web site.

20. E-safety Group/Governor

We are in the process of setting up an E-safety Group to develop all aspects of E-safety at Sandown following a detailed review of our E-safety provision. The Governor with responsibility for monitoring E-Safety activities at Sandown School is Seb Gore.

21. Appendices

- Appendix 1 – E-Safety Rules for Key Stage 1.
- Appendix 2 – E-Safety Rules for Key Stage 2.
- Appendix 3 – Parents' Acceptable Use Agreement.
- Appendix 4 – Pupils' Acceptable use Agreements.
- Appendix 5 – Staff Acceptable Use Policy.
- Appendix 6 - E-safety incident flow charts for children and staff.

Key Stage 1

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 should only 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.



Key Stage 2

Think then Click

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we not sure about.
- We only e-mail people an adult has approved.
- We send e-mails 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 e-mails sent by anyone we don't know.
- We do not use Internet chat rooms.

Sandown Primary School E-Safety Policy Appendix 3

Parents' Acceptable Use Agreement

These E-Safety Rules help to protect pupils and the school by describing the acceptable and unacceptable computer use of school computing equipment and resources.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school computing systems may not be used for private purposes, unless the Headteacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer 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.

Sandown Primary School E-Safety Policy Appendix 3: continued.....

Parents' Acceptable Use Agreement

Our School E-Safety Rules

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

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.

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

Sandown Primary School E-Safety Policy Appendix 4

Pupils' Acceptable Use Agreements

School Policy

Digital technologies have become integral to the lives of children and young people, both within school and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

These Acceptable Use Agreements are intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

Sandown Primary School E-Safety Policy Appendix 4: continued.....

For Children in Reception to Year 4 - Younger Children

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers.

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment.

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):.....

Date:.....

Sandown Primary School E-Safety Policy Appendix 4: continued.....

For Children in Years 5 and 6 – Older Children

E-Safety Pupils Acceptable Use Policy Personal Agreement: Page 1

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my usernames and passwords safe and secure - I will not share them, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If should never arrange to meet people off-line that I have communicated with on-line, however, if I do then I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube.)

Sandown Primary School E-Safety Policy Appendix 4: continued.....

For Children in Years 5 and 6 – Older Children

E-Safety Pupils Acceptable Use Policy Personal Agreement: page 2

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

- I will only use social media sites with permission.

Sandown Primary School E-Safety Policy Appendix 4: continued.....

For Children in Years 5 and 6 – Older Children

E-Safety Pupils Acceptable Use Policy Personal Agreement: Page 3

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read (or had read through to you by an adult), understood and agree to the rules included in the Acceptable Use Agreement.

If you do not sign and return this agreement, access will not be granted to school systems and devices.

Sandown Primary School E-Safety Policy Appendix 4: continued.....

For Children in Years 5 and 6 – Older Children

E-Safety Pupils Acceptable Use Policy Personal Agreement: Page 4

Pupil Acceptable Use Agreement Form

This form relates to the pupil Acceptable Use Agreement, to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school).
- I use my own devices in the school (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil

Year Group + Class

Signed

Date

Sandown Primary School E-Safety Policy Appendix 5: Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should refer to the school's E-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure 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 school E-Safety Co-ordinator or the Designated Safeguarding Lead (DSL).
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of 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 agree with the Information Systems Code of Conduct

Signed: Capitals: Date:.....

Accepted for school: Capitals.....

Status:..... Date:

Sandown Primary School E-Safety Policy Appendix 6:

E-safety incident flow charts for Children and Staff

E-safety incident ?

If you see something which
upsets you



Stop



Leave your screen as it is
Don't shut down



Tell a grown up straight away



You're not in trouble; it's not
your fault

Sandown Primary School E-Safety Policy Appendix 6: continued.....

