West Pennard
CE Primary School

E-Safety Policy

Our school vision…

'Since God so loved us, so we must love one another'
(1 John 4 v11)

Valuing our Christian foundation, we care for each other and our world.
We develop resilience, confidence, creativity and independence through our innovative and diverse curriculum; inspiring and motivating everyone to thrive.
Our motto, 'To Try is to Triumph' and growing Christian Values, are central to all that we do.

We link this policy with our Christian values of:

- **Truthfulness**
- **Compassion**
- **Friendship**
- **Thankfulness**
- **Respect**
- **Forgiveness**

We are fully committed to each day a fresh start in the spirit of forgiveness and Christian love.

Introduction

West Pennard Primary School fully recognises the contribution it can make to protect children and support them in school. The aim of this policy is to safeguard and promote our pupils' safe use of internet and electronic communication technology such as mobile phones and wireless connectivity.

This policy highlights the need to educate children and young people about the benefits and risks of using new technologies both in and away from school.

It also provides safeguards and rules to guide staff, pupils and visitors in their online experiences.

The school e-safety policy relates to other policies including those for Computing, anti-bullying and for child protection.

Effective Practice in e-Safety

E-Safety depends on effective practice in each of the following areas:

- Education for responsible computing use by staff and pupils;
- A comprehensive, agreed and implemented e-Safety Policy;
- Secure, filtered broadband from the SWGfL;
- A school network that is compliant with National Education Network standards and specifications.

Writing and reviewing the e-safety policy

The e-Safety Policy is part of the School Development Plan and relates to other policies including those for Computing, anti-bullying and for child protection.

E-Safety Co-ordinator: Tony Wheat (Computing Co-ordinator)
Designated Senior Person for Child Protection: Jo Hale (Head Teacher)

- Our e-Safety Policy has been written by the school and is based on the Kent e-Safety Policy. It has been agreed by senior management and approved by governors.
- It was approved by the Governors on: …
- The next review date is: …

Teaching and learning

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 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. This includes the use of SWGfL Firewall, the ability to block/limit internet access to users/areas, Sophos Virus Protection.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use through discussion and signing of the e-safety contract on an annual basis.
- 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 shown how to publish and present information to a wider audience and how to evaluate Internet content.

Pupils will be taught how to evaluate Internet content

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

- Pupils will be taught the importance of cross-checking information before accepting its accuracy and how to report unpleasant Internet content both in school, through the class teacher / Computing technician, or at home using 'report' buttons.

Managing Internet Access

Information system security

- School computing systems security will be reviewed regularly.
- Sophos Virus protection will be updated regularly through automatic updates.

E-mail / messaging

- Pupils are discouraged from using e-mail accounts or social media on the school system, unless it forms part of a lesson or series of lessons.
- Pupils must immediately tell a teacher if they receive offensive messages.
- In online communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Messages from pupils to external bodies is controlled carefully by the class teacher or teacher supervising the activity.
- Teachers must not send, receive or check emails during lesson time.

Published content and the school web site

- Staff or pupil personal contact information will not be published.
- The Headteacher and Computing Co-ordinator will take editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Parents sign an authorisation form (Data/Image Protection) when their child joins West Pennard, giving permission for images of their child (or their work) to be used on the website and on other publications. Where this permission is not granted, photos/work are never used.
- Photographs that include pupils will be selected appropriately to avoid images being misused. Although pupils may be recognised, photos used on the website are low-quality, and if required, edited to prevent children without photographic consent being identified.
- Pupils surnames will not be used anywhere on the school website or other on-line space in association with photographs or video, unless express permission has been granted by parents/carers.
- Work published on the website will not be identified with an individual pupil.
- Pupil image file names will not refer to the pupil by name.
- Parents/carers are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing

- The access to social networking sites is controlled through the SWGfL filtering. The facility to

unblock Social Networking sites for individual schools exists, and we have the ability to do so at the request of the class teacher and approval of the Computing co-ordinator or Head Teacher.

- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Ideally pupils would use only moderated social networking sites and older pupils will be educated on their safe use.
- Sites such as Snapchat and Facebook etc. should **NOT** be used.
- 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 avatars when using social networking sites.
- Parents E-Safety 'Seminars' will be offered to all parents concerned about the issues of internet use within school and at home.

Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to Computing Coordinator. Sites can be referred to the SWGfL team for global blocking if required, or local blocking can be performed on-site.

Managing videoconferencing & webcam use

- Pupils must ask permission from the supervising teacher before making or answering a videoconference call, or communicating by way of VOICP, such as Skype.
- Video-conferencing and webcam use will be appropriately supervised for the pupils age.

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.
- Mobile phones with wireless Internet access can bypass school filtering systems and present an alternative route to undesirable material and communications. Pupils at West Pennard are not permitted to have mobile phones in school.

Staff Use of personal Mobile Phones/cameras

- Staff are discouraged from taking personal mobile phones on trips. Emergency calls, where necessary should be through the use of the office mobile phone and go through the school office.
- Staff are **only** to make and receive calls and / or text messages outside of lesson time and **never** within the earshot of pupils or parents.
- Mobile phones must be turned off or on 'silent' during lesson time, in staff meetings and on INSET days.
- School digital cameras are available. Staff are encouraged to download images in school.

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

- All staff must read and sign the staff 'e-safety contract' before using any school Computing resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- Parents will be asked to sign the 'e-safety contract' for their child to use the internet as part of the induction process. Children are asked at KS2 to counter-sign the 'e-safety contract' after discussion with parents/carers.
- Any person not directly employed by the school will be asked to accept the 'e-safety contract' before being allowed to access the internet from the school site.
- All users of the school computer system understand that the systems in place afford no privacy.

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 Somerset LEA can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit computer use on a regular basis to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective through informal/formal monitoring.

Handling e-safety 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 and LA Child Protection Procedures.
- If a serious breach of the 'e-safety contract' is discovered, the monitor of the PC in question should be turned off and the computer put 'out of order'. This is to prevent the contamination of evidence that may be collected by outside agencies (e.g. police) if required.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Community use of the Internet

- Any use of the school system by visitors will be bound by the terms and conditions in the 'e-safety contract' and will be monitored by the systems in place for pupils and staff.

Communications Policy

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.
- E-Safety training will be embedded within the Wessex scheme of work and the Personal Social and Health Education (PSHE) curriculum.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Any staff member with an online identity' (e.g. in social networking sites) will ensure that access to this information is kept private and not shared with pupils at West Pennard Primary School.
- Staff will always use the 'safe search' facilities within search engines when accessing the web with pupils and must check all search terms before use with pupils.

Enlisting parents' and carers' support

- West Pennard Primary School's E-Safety Policy will be shared with parents and carers in the school welcome pack and on the school web site.
- Parents with any concerns about E-Safety are encouraged to contact the school for further guidance and support.
- Parents sign the Parent's 'e-safety contract' on an annual basis after sharing our age appropriate safety rules with their child (see appendix 3)

Appendix 1: Useful resources for teachers

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

Becta
http://schools.becta.org.uk/index.php?section=is

Chat Danger
www.chatdanger.com/

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

Childnet
www.childnet-int.org/

Cyber Café
http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen

www.digizen.org/

Kent e-Safety Policy and Guidance, Posters etc
www.clusterweb.org.uk/kcn/e-safety_home.cfm

Kidsmart
www.kidsmart.org.uk/

Kent Police – e-Safety
www.kent.police.uk/Advice/Internet%20Safety/e-safety%20for%20teacher.html

Leicestershire Constabulary – Internet Watch Foundation
www.leics.police.uk/advice/2_information_zone/50_internet_watch_foundation

Think U Know
www.thinkuknow.co.uk/

Safer Children in the Digital World
www.dfes.gov.uk/byronreview/

Appendix 2: Useful resources for parents

Care for the family
www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD
http://publications.teachernet.gov.uk

Family Online Safe Institute
www.fosi.org

Internet Watch Foundation
www.iwf.org.uk

Kent leaflet for parents: Children, ICT & e-Safety
www.kented.org.uk/ngfl/ict/safety.htm

Parents Centre
www.parentscentre.gov.uk

Internet Safety Zone

Appendix 3:

West Pennard Primary School

ACCEPTABLE INTERNET USE STATEMENT

Parents/Guardians of pupils should sign a copy of this Acceptable Internet Use Statement and return it to the school where it will be countersigned by a member of staff. Failure to read and complete this form will restrict the use of the computers in school for your child. ***Thank you for your co-operation.***

The computer system is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management. The school has an Internet Access Policy drawn up to protect all parties - the pupils, the staff and the school.

The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet sites visited.

- Access should only be made via the authorised account and password that should not be made available to any other person.
- The security of the IT system must not be compromised whether owned by the school, by Somerset Council or any other organisation or individual.
- Sites and materials accessed must be appropriate to work in school. Users will recognise materials that are inappropriate and should expect to have their access removed.
- Users are responsible for all messages sent and for contacts made that may result in e-mail being received.
- The same professional levels of language and content should be applied as for letters or other media, particularly as e-mail is often forwarded.
- Posting anonymous messages and forwarding chain letters is forbidden.

- Cyber bullying, using abusive and unkind comments is forbidden.
- Copyright of materials and intellectual property rights must be respected.
- All Internet use should be appropriate to staff professional activity or to student's education. However please note that:-
    - The school's computing system may be used for private purposes following guidelines established by the school.
    - Use for personal financial gain, gambling, political purposes or advertising is forbidden.
    - Closed discussion groups can be useful but the use of public chat rooms is not allowed.
    - Pupils' irresponsible use of the internet will result in temporary/permanent exclusion of use.

Members of staff are reminded that they should not deliberately seek out inappropriate/offensive materials on the Internet and that they are subject to the LA's recommended disciplinary procedures should they do so. This includes on school owned property (laptops) used at home.

Child's name _____

Signed _____ date _____
(parent/guardian)

Approved _____ date _____
(Head/class teacher)

West Pennard Primary School

E- Safety Rules

These rules help us to stay safe on the Internet

- ☺ **I will keep my own passwords a secret and will not tell anyone what they are.**
- ☺ **I will not use the computers in school to send or receive e-mails or other messages unless told I can do so by my teacher or another member of staff.**
- ☺ **The messages I send will be polite and sensible; I will not send messages using abusive, inappropriate or unkind comments.**
- ☺ **To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive a message I do not like; I will not respond to abusive messages.**
- ☺ **I will not give my home address or phone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;**
- ☺ **I will not give out personal contact details online or post photographs of myself on sites.**
- ☺ **I will only visit websites or click on the links I have been told to, unless searching the internet.**
- ☺ **I will not visit any social networking sites or online games, such as Youtube, Facebook or Snapchat.**
- ☺ **I understand that the school can check my computer files and the Internet sites I visit.**

I have read, understood and accept the e-safety rules for West Pennard School.

Signed: …… Capitals: …… Date: ……

Appendix 4:

West Pennard Primary School

Staff Code of Conduct for Computing

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 Computing system for a purpose not permitted by its owner.

- I appreciate that Computing includes a wide range of systems, including mobile phones, digital cameras, email, social networking and that computer use may also include personal computing 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 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 Safeguarding Lead in the school (Jo Hale).

- I will ensure that electronic communications with pupils and / or parents including email, IM and social networking are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.

- I will ensure that I only use my mobile phone to communicate with others outside of lesson time and out of the earshot of pupils and parents.

- I will ensure that my mobile phone is switched off or on 'silent' during lesson time, in staff meetings and on INSET days.

- I will not send, receive or check emails during lesson time.

- I will promote e-safety with pupils 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, 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 Computing.

Signed: …… Capitals: …… Date: ……

Accepted for school: …… Capitals: ……