Western Downland C.E. Primary School
In partnership with parents we aim to provide:
'The roots to grow and the wings to fly'

Western Downland C.E. (Aided) Primary School

Keeping Children Safe in using ICT (Online Safety Policy)

Date approved: May 2016
Review date: May 2017

MISSION STATEMENT

In partnership with parents we aim to give children: 'The roots to grow and the wings to fly'.

A place where:

- everyone is valued and has the opportunity to succeed.
- learning is the highest item on the agenda for children and adults.
- the Christian values of kindness, consideration and forgiveness shape our community.
- pupil learning and school improvement will be achieved in partnership with Governors, Staff, Parents and Pupils.
- involvement will be educationally and spiritually uplifting.

1. Statement of Intent

Children interact with the Internet and other communications technologies such as mobile phones on a regular basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas and social interaction is greatly beneficial but can occasionally place young people in danger.

This policy aims to ensure there is the right balance between controlling access to technology, setting rules and educating children for responsible use. Online safety comprises all aspects relating to children and their safe use of the internet and other technologies. It includes raising awareness of the risks and is part of the "Duty of Care" which applies to everyone working in children's education.

Our Online Safety Policy has been written by the school, building on guidance from HCC and Becta (the Government agency with responsibility for effective and safe use of technology.) and should be read alongside our other Safeguarding Policies, our policy on Staff Acceptable use of ICT and our School Social Media Policy. The Online Safety Policy will be reviewed **annually** by staff and Governors.

2. Teaching and Learning

a) The importance of Internet use.

- The purpose of children's 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 business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and children.
- Internet access is an entitlement for children where a responsible and mature approach to its use is shown.
- The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience.
- Children 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.

b) How the Internet benefits education.

Benefits of using the Internet in education include:-

- access to world-wide educational resources e.g. museums and art galleries;
- educational and cultural exchanges between pupils world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with the LA and the DCSF;
- access to learning wherever and whenever convenient.

c) How the Internet can enhance learning.

- The school Internet access will be designed expressly for children use and will include filtering appropriate to the age of the children and needs of learning.

- Children will be taught what Internet use is acceptable and what is not and given clear objectives for internet use, using the e-safety framework curriculm objectives.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed regularly to reflect the curriculum requirements and age of children.
- Staff should guide children in on-line activities that will support the learning outcomes planned for their children's age and maturity.
- Children will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

d) How children learn to evaluate Internet content.

- If staff or children discover unsuitable sites, the URL (address), time date and content must be reported to IT co-ordinator (Mrs Jondelle Barftlett) or via the Online safety co-ordinator (Kim Wilcox,the headteacher.)
- Schools should ensure that the use of the Internet derived materials by staff and by children complies with copyright law.
- Children should be taught to be critically aware of the materials they read and shown how to validate information before accepting it accuracy.
- Children will be taught to acknowledge the source of information used and to respect copyright when using the Internet material in their own work.

3. Managing Internet Access

a) Maintaining ICT system security.

- The security of the school ICT systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the LA.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Portable media may not be used without specific permission.
- Unapproved system utilities and executable files will not be allowed in children's work areas or attached to e-mail.
- Teachers keep a vigilant view in lessons of sites accessed by children. Children are not allowed to access the internet without direct adult supervision.The IT co-ordinator will review system capacity annually.

b) Management of e-mail

- Children may only use approved e-mail accounts on the school system.
- Children must immediately tell a teacher if they receive offensive e-mail.
- Children must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Whole- class or group e-mail addresses should be used only (not individual).
- Access in school to external personal e-mail accounts is not permitted
- Social e-mail is not permitted
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

c) Management of published content

- The content details on the Web site should be the school address, e-mail and telephone number. Staff or children's personal information will not be published.
- E-mail addresses should be published carefully, to avoid spam harvesting.

- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidance for publications including respect for intellectual property rights and copyright.

d) Publishing images of children or their work

- Photographs that include children will be selected carefully and will not enable individual children to be clearly identified.
- Children's full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of children are published on the school Web site.
- Children's work can only be published with the permission of the children and parents.

e) Management of collaboration tools.

- Newsgroups will not be made available to children unless an educational requirement for their use has been demonstrated.

f) Management of social networking and personal publishing.

- Access to social networking sites is not permitted and HCC filters are in place.
- Children are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, e-mail address, names of friends, specific interests and clubs etc.
- Children are 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 child or his/her location eg. House number, street name, school, shopping centre.
- Teachers' blogs or wikis should be password protected and run from the school website. Teachers are advised not to run social network spaces for children on a personal basis.
- Children should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications.
- Children should be advised not to publish specific and detailed private thoughts.
- Staff should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

g) Managing filtering.

- The school will work in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems to protect children are reviewed and improved.
- Filtering is managed by Hampshire LA (Hants IT) and the IT co-ordinator (Jondelle Bartlett)
- Headteacher staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Any material that the school believes is illegal must be referred to the Headteacher
- Filtering strategies will be selected by the school, in discussion with the filtering provider where appropriate. The filtering strategy will be selected to suit the age and curriculum requirements of the children.

h) Management of video conferencing.

- Video conferencing is presently not undertaken by the school.

i) Management of 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 will **not** be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

j) Personal data protection.

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

4. Policy Decisions

a) Authorisation of Internet access.

- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- At Key Stage 2, children will be provided with supervised Internet access.
- Primary pupils will not be issued individual e-mail accounts, but may be authorised to use a group/class e-mail address under supervision if appropriate to the curriculum.

b) Risk Assessment

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for children. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor HCC can accept liability for the material accessed, or any consequences of Internet access.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The headteacher will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.

c) Online safety complaints.

- Complaints of Internet misuse will be dealt with the headteacher.
- Any complaint about staff misuse must be referred to the headteacher.
- Children and parents will be informed of the complaints procedure.
- Parents and children will need to work in partnership with staff to resolve issues.
- Discussions will be held with the Police Liaison Officer to establish procedures for handling potentially illegal issues.

d) Internet use across the community.

- The school will be sensitive to Internet related issues experienced by children out of school, e.g. social networking site, and offer appropriate advice.

5. Communications Policy

a) Pupils

  - Rules for Internet access will be displayed in classrooms at the junior site.
  - Children will be informed that Internet use will be monitored.
- There is a programme of Online Safety training used to raise the awareness and importance of safe and responsible internet use (using the Online safety framework curriculum

programme), including specific safeguarding issues, appropriate to the children's age, such as radicalisation, online grooming, online bullying and sexting.

- Instruction in responsible and safe use should precede Internet access.
- Responsible Internet use is included in the school's curriculum.

b) Staff

- All staff must read the staff acceptable use of ICT and sign to accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- All staff will be given the School Online Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user- spot check will be carried out.
- Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
- Staff development in safe and responsible Internet use and on the school e-Safety Policy will be provided as required, including specific safeguarding issues such as radicalisation and on-line grooming.

c) Parents

- Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school Web site.
- Internet issues will be handled sensitively to inform parents without alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical and suggestions for safe home Internet use.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents twice a year.
- Interested parents will be referred to organisations listed in Appendix 1 "Online Safety Contacts and References."

Appendix 1.

Online Safety Contacts and References

Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk/contact us.htmt

Think U Know website
http://www.thinkuknow.co.uk?

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

Internet Watch Foundation
http://www.iwf.org.uk/

Internet Safety Zone
http://www.internetsafetyzone.com/

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

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

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

Stop Text Bully
www.stoptextbully.com

NCH – The Children's Charity
http://www.nch.org.uk/stories/index.php?i=324

NCH – Digital Manifesto
http://www.nch.org.uk/uploads/documents/Digital Manifesto web.pdf

BBC Chat Guide
http://w.bbc.co.uk/chatguide/

Childnet
www.childnet.com

Appendix 2.

Notes on the legal framework

An awareness of legal issues is important, but this page is not a definite 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 include:

- The 2003 Sexual Offenders Act has introduced new offences of Grooming and raised the age for making/distributing indecent images of children to 18.
- Offences regarding racial hatred are covered by the Public Order Act 1986 although a new Racial and Religious Hatred Bill is going through parliament.

Possible offences:
Sexual Offences Act 2003

- Grooming – If you are over 18 and have communicated with a child under 16 at least twice (including by phone or 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.
- Making indecent images – it is an offence to take, make, distribute, show, advertise indecent images of a child under 18. (NB to view an indecent image on your computer means that you have made a digital image).
- Causing a child under 16 to watch a Sexual Act – to intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.
- Abuse of positions of trust – Staff must be aware that it is 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. (Applies to teachers, social workers, health professionals, connexions staff)

N.B. Schools should already have a copy of 'Children & Families: Safer from Sexual Crime' document as part of their child protection packs.
Information about the 2003 Sexual Offences Act can be found at www.teachernet.gov.uk

Relevant Legislation
The Computer Misuse Act 1990 – makes it a criminal offence to gain access to a computer without permission. The motivation could be the technical challenge, date theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.
Public Order Act 1986 – offence to possess, publish disseminate material intended to /likely to incite racial hatred.
Communications Act 2003 – There are 2 separate offences under this act:

a) sending by means of a public electronic communications network, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character.
b) sending of a false message or persistently making use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety.

This wording is important because the offence under a) is complete when the message has been sent – no need to prove any intent or purpose. It is an offence under b) to keep using the network for sending any kind of message irrespective of content if for the purpose of causing annoyance etc.
Malicious Communications Act 1988 – offence to send a letter, electronic communication or article which is indecent or grossly offensive, threatening or false information with intent to cause distress or anxiety to the recipient.
Copyright, Design and Patents Act 1988 – it is an offence to use unlicensed software.
Protection of Children Act 1978 – The law on images of child abuse is clear. It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom.
Obscene Publications Act 1959 and 1964 – defines "obscene" and related offences.
Protection from Harassment Act 1997
Section 2 – 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.
Section 4 - 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.
***Keeping Children Safe in Education* 2015 : DfE July 2015**

Monitoring School ICT Use

Monitoring network activity could contravene Article 8 of the European Convention of Human Rights and Fundamental Freedoms, e.g. the right to respect for private and family life, which is protected by the Human Rights Act 1998.
The Telecommunications (Lawful Practice) (Interception of Communications) Regulations 2000 also limit monitoring. The 2000 Regulations apply to all forms of electronic monitoring and interception irrespective of whether the material monitored is generated by private use or in the course of the school's day to day activities.
A school may only monitor authorised private use of a computer system if it can justify monitoring on the basis that it is lawful, necessary and in the interest of amongst other things, the protection of health or morals or for the protection of the rights and freedoms of others. Schools should ensure that the monitoring is not out of proportion to the harm that could be done if the monitoring did not take place.
Schools could start by banning private use of the network, but then allow private use following application to the Headteacher. The Rules for Responsible Internet Use, with which every user agrees to comply, contains a paragraph that should ensure users are aware that the school is monitoring Internet use.
In order to defend claims that it has breached either the 2000 Regulations or the Human Rights Act 1998, a school should devise procedures for monitoring, ensure monitoring is supervised by a senior manager and maintain a log of that monitoring.

Sex Offences Act 2003 Memorandum of Understanding

Memorandum of Understanding Between Crown Prosecution Service (CPS) and the Association of Chief Police Officers (ACPO) concerning Section 46 Sexual Offences Act 2003.
The aim of this memorandum is to help clarify the position of those professionally involved in the management, operation or use of electronic communications networks and services who may face jeopardy for criminal offences so that they will be reassured of protection where they are acting to combat the creation and distribution of images of child abuse. This memorandum has been created within the context of child protection, which will always take primacy.
For the MOU: http://www.iwf.org.uk/police/page.22.213.htm