

**WEST HILL PRIMARY SCHOOL
SCHOOL ONLINE SAFETY POLICY and INTERNET CODE OF CONDUCT
April 2017**

Date of Review	Body responsible for review of Statutory Policies	Date of next review
27.4.17	FGB	Summer 2020
	FGB	

This policy has 'Safeguarding Children and Child Protection', the school's 'Healthy school', 'Investors in People Gold', 'Forest School' and 'Artsmark Gold' ethos', 'Excellence and Enjoyment' and the School's Mission Statement and Aims at its heart.

West Hill Primary School is a Co-operative Trust school having formed The SMILE Learning Trust in November 2013.

(Support, Motivate, Inspire, Learn, Excel)

Our school ethos is based on 'Care', 'tolerance', 'trust' and 'respect' and on our SMILE Learning Trust Co-operative Values of: self-help, self-responsibility, democracy, equality, equity, solidarity. As Co-operative members, we believe in the ethical values of honesty, openness, social responsibility and caring for others,

and on the British Values of

Respect (including respect for beliefs, faiths, cultures and the environment), Tolerance, Democracy, The Rule of Law, Individual Liberty, Tradition and Heritage.

Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. A school online safety policy should help to ensure safe and appropriate use. The development and implementation of our policy involves all the stakeholders in a child's education from the headteacher and governors to the senior leaders and classroom teachers, support staff, parents, members of the community and the pupils themselves.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Online-bullying

- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies (eg. behaviour, anti-bullying and child protection policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks. It is important that the school, as well as parents, adopt strategies for the responsible and safe use of the Internet.

Some of the material is published for an adult audience and is unsuitable for pupils. In addition, some use the Web to publish information on weapons, crime and racism that would be more restricted elsewhere. Sadly e-mail and chat communication could also provide opportunities for adults to make contact with children for inappropriate reasons. In line with school policies that protect pupils from other dangers, there is a requirement to provide pupils with as safe an Internet environment as possible and a need to teach them to be aware of and respond responsibly to the risks.

Schools need to protect themselves from possible legal challenge. The legal system is still struggling with the application of existing decency laws to computer technology. It is clearly an offence to hold images of child pornography on computers but the possession of other obscene or offensive materials is not clearly covered. The Computer Misuse Act 1990 makes it an offence to "cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer". Schools can help protect themselves by making it clear to users that the use of school equipment to view or transmit inappropriate material is "unauthorised". However, schools should be aware that a disclaimer does not protect a school from a claim of death or personal injury and the school needs to ensure that all reasonable and appropriate steps have been taken to protect pupils.

Government guidance in areas such as e-mail, chat and websites has changed recently. West Hill Primary School has copies of the DfES Superhighway Safety pack (green cover) and has noted the additional guidance on the Web site: <http://safety.ngfl.gov.uk> West Hill Primary School also adheres to safety guidance promoted by the SWGfL via the website: <http://www.swgfl.org.uk/Staying-Safe> and through annual conferences.

The school's policy has been revised in the light of government guidance and of the fact that Internet technology and school use is changing rapidly. It will be reviewed annually, or more often should changes to Internet use cause concern.

Development/Monitoring/Review of this Policy

This Online Safety policy has been developed by:

- *School Online safety Coordinator – Mrs. Hudson*
- *Headteacher / Senior Leaders*
- *Teachers*
- *Support Staff*

WEST HILL PRIMARY SCHOOL
SCHOOL ONLINE SAFETY POLICY and INTERNET CODE OF CONDUCT
April 2017

- *Governors*
- *Parents*

Consultation with the whole school community has taken place through the following:

- *Staff meetings*
- *School Council / pupils*
- *Governors meeting*
- *Parents evening*

Schedule for Development/Monitoring/Review

This online safety policy was approved by the <i>Governing Body</i> on:	<i>Insert date: 27/4/2017</i>
The implementation of this online safety policy will be monitored by the:	<i>Online safety Coordinator, Senior Leadership Team, The School Council/ Digital Leaders</i>
Monitoring will take place at regular intervals:	<i>Following annual safety briefings</i>
The <i>Governing Body</i> will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	<i>With the annual Computing report to the Governors</i>
The Online safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	<i>April 2018</i>
Should serious online safety incidents take place, the following external persons / agencies should be informed:	<i>LA Online Safety Manager, LA Safeguarding Officer, Police Commissioner's Office (advice maybe sought from SWGfL team)</i>

The school will monitor the impact of the policy using:

- *360° Degree Safe – reviewed annually*
- *Logs of reported incidents*
- *SWGfL monitoring logs of internet activity (including sites visited)*
- *Internal monitoring data for network activity*
- *Surveys / questionnaires of*
 - *students / pupils (eg Ofsted “Tell-us” survey / CEOP ThinkUknow survey)*
 - *SWGfL Surveys*
 - *parents / carers*
 - *staff*

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Considerations for West Hill Primary School

Supervision is the key strategy. Whatever systems are in place, something could go wrong which places pupils in an embarrassing or potentially dangerous situation. It is not sufficient for a teacher or learning support assistant to be in the area. Circumstances outside normal lesson time where pupils justifiably need access to the Internet will be fully supervised.

Aimless surfing is never allowed. Pupils will be taught to use the Internet in response to an articulated need – e.g. a question arising from work in class. Children should be able to answer the question “Why are we using the Internet?”

In addition, West Hill Primary School has banned the use of mobile phones by pupils in school. (Special arrangements can be made for keeping phones in the office during school hours, should the need arise) In accordance with the Education Act 2012, the school reserves its right to search for a phone if it is believed a pupil is using it inappropriately.

Examples of effective Internet use have been devised by many infant and junior schools and examples may be found for reference on the Kent NGfL Web site www.kented.org.uk/ngfl.

Search engines can be difficult to use effectively and pupils can experience overload and failure if the set topic is too open-ended. Teachers will choose a topic with care, select the search engine and then discuss with pupils sensible search words (which have been tried out beforehand!). This will lead to a fruitful group or class investigation as opposed to possible individual frustration.

Pupils do not need a thousand Web sites on weather. A small selection is quite enough choice for juniors. Learning Resources or RM Tutor can be used to limit the sites pupil’s have access to in any given lesson. Teachers’ Web site selections for various topics can be put on the school Web site. This enables access by pupils from home.

There may even be difficulties here. One recommended site, successfully used by primary schools, suddenly changed into a pornographic site. Presumably hackers had infiltrated the site and replaced the content. Sites should always be previewed.

Off-line storage of Web resources for viewing later from the hard disk is one useful strategy. Similarly pupils publishing to a web site held on a class computer or the school network removes difficulties of pupils publishing on a publicly available Web site and could still be presented to pupils as a privilege.

Government advice on e-mail has changed. The concern is the possibility of access to pupils by adults of unknown intention, if e-mail is not controlled. Essentially individual e-mail addresses are not considered suitable and class or project e-mail addresses are used at the school.

In brief, we, at West Hill Primary School:

- Adhere to the guidance in the DfE Superhighway Safety Pack, and SWGfL websites
- Check the e-mail, chat and Web site updates on <http://safety.ngfl.gov.uk>. And <http://www.swgfl.org.uk/Staying-Safe>

- Discuss and review with pupils the Rules for Responsible Internet Use.
- Teach Internet Safety using CEOP, NSPCC, SWGfL material as appropriate.
- Consider class e-mail addresses and check all incoming and outgoing e-mail.
- Preview all sites before use and consider off-line viewing.
- Plan the curriculum context for Internet use to match pupils' ability.
- Vigilance is essential and supervision the most important strategy.

Core Principles of Internet Safety

The Internet is becoming as commonplace as the telephone or TV and its effective use is an essential life-skill. Unmediated Internet access brings with it the possibility placing of pupils in embarrassing, inappropriate and even dangerous situations. This policy helps to ensure responsible use and the safety of pupils.

West Hill Primary School Use of the Internet Policy, based on the Kent NGfL and Devon SWGfL Internet Policies, is built on the following five core principles:

Guided educational use

Significant educational benefits should result from curriculum Internet use including access to information from around the world and the abilities to communicate widely and to publish easily. Internet use should be planned, task-orientated and educational within a regulated and managed environment. Directed and successful Internet use will also reduce the opportunities for activities of dubious worth.

Risk assessment

21st Century life presents dangers including violence, racism and exploitation from which children and young people need to be protected. At the same time they need to learn to recognise and avoid these risks – to become “Internet Wise”. Our school needs to ensure they are fully aware of the risks, needs to perform risk assessments and to implement its policy for Internet use. Pupils need to know how to cope if they come across inappropriate material.

Assessments of the risks in Internet access by young persons in Youth Clubs, Libraries, public access points and in homes will need to be undertaken.

Responsibility

Internet safety depends on staff, schools, governors, advisers, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and associated communication technologies. The balance between education for responsible use, regulation and technical solutions must be judged carefully.

Regulation

The use of a limited and expensive resource, which brings with it the possibility of misuse, must be regulated. In some cases access within the school must simply be denied, for instance unmoderated chat rooms present immediate dangers and are banned. Fair rules, clarified by discussion and prominently displayed help pupils make responsible decisions.

Appropriate strategies

This document describes strategies to help to ensure responsible and safe use. They are based on limiting access, developing responsibility and on guiding pupils towards educational activities. Strategies are selected to suit the school situation and their effectiveness monitored by staff. There are no straightforward or totally effective solutions and staff, parents and the pupils themselves must remain vigilant.

Policy Statement

The Internet and Online Safety Policy is part of the Computing Policy and School Development Plan and relates to other policies including those for behaviour and discipline, for personal, social and health education (PSHE) and for citizenship. The construction and regular revisiting of this Policy provides a method to review practice, in this case the use of a major new technology with benefits and risks.

Our Internet Policy has been written by the school, building on Devon, Kent and government guidance. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

Roles and Responsibilities:

Governors: The Online Safety Governors will be Mr. J. Brook, Computing Lead Governor and Mrs. J. Meredith and Mr. I. Heard as part of their Safeguarding Children roles.

Mrs. Meredith's and Mr. Heard's role will be to report to relevant governors meetings.

Headteacher and Senior Management Team

The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community. The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See SWGfL flowchart)

Computing Technician and Computing Subject Leader are responsible for ensuring

- that the school's Computing infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the online safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority Online Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed

Teaching and Support Staff are responsible for ensuring:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy / Agreement (AUP)

- they report any suspected misuse or problem to the Online safety Co-ordinator / Headteacher / Senior Leader / Head of ICT / Computing Subject Leader or Class teacher for investigation / action / sanction
- digital communications with pupils should be on a professional level

Pupils are responsible for using the school Computing systems in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign annually before being given access to school systems.

Parents / Carers / Teachers will be responsible for

- endorsing (by signature) the Pupil Acceptable Use Policy
- accessing the school website / on-line pupil records in accordance with the relevant school Acceptable Use Policy. (When appropriate)

Designated person for child protection/Child Protection Officer

Are trained in online safety issues and are aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online-bullying

Education & Training- Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies
- The Online Safety Coordinator (or other nominated person) will receive regular updates through attendance at SWGfL / LA / other information / training sessions and by reviewing guidance documents released by SWGfL / LA and others.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The Online Safety Co-ordinator (or other nominated person) will provide advice / guidance / training to individuals as required.

Training- Governors

Governors should take part in online safety training / awareness sessions through participation in school training or information sessions for parents.

The Importance of the Internet

West Hill Primary School Policy Statements

- The purpose of Internet use at West Hill Primary 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 pupils.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- 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.

At West Hill Primary School Online Safety education will be provided in the following ways:

- A planned online safety programme will be provided as part of Computing/ PSHE / other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school

- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information

Pupils and staff will also have:

- access to world-wide educational resources including museums and art galleries;
- inclusion in government initiatives such as the National Grid for Learning (NGfL) and the Virtual Teacher Centre (VTC);
- 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;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- exchange of curriculum and administration data with the LA and DfE.

How Internet use will enhance learning

West Hill Primary School Policy statements:

- 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 is acceptable and what is not acceptable and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location and retrieval.
- Pupils will be taught how to report unacceptable or abusive material.

How pupils will learn to evaluate Internet content

West Hill Primary School Policy Statements:

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing Subject Leader.
- The School ensures that the use of Internet derived materials by staff and by pupils complies with copyright law.

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.
- Training will be available to staff in the evaluation of Web materials and methods of developing students' critical attitudes.

How e-mail will be managed :

West Hill Primary School Policy Statements:

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- Whole-class or group e-mail addresses are used in the school.
- Access in school to external personal e-mail accounts will be blocked.
- Social e-mail use can interfere with learning and will be restricted.
- 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 banned.

How Web site content will be managed.

West Hill Primary School Policy statements:

- The point of contact on the Web site should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
- Web site photographs that include pupils will be selected carefully and will not enable individual pupils to be identified.
- Pupils' full names will not be used anywhere on the Web site, particularly associated with photographs.
- When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
- The headteacher or nominee will take overall editorial responsibility and ensure content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

Conferencing and chat.

West Hill Primary School Policy Statements:

- Pupils will not be allowed access to public or unregulated chat rooms.
- Children should use only regulated educational chat environments. This use will always be supervised and the importance of chat room safety emphasised.
- Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.
- A risk assessment will be carried out before pupils are allowed to use a new technology in school.

How can emerging Internet uses be managed?

West Hill Primary School Policy Statements:

- 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 photographic images, abusive or inappropriate text messages is forbidden.
- Children will not use tablets and other similar devices brought from home.

Authorisation of Internet Access.

West Hill Primary School Policy Statements:

- The school will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff leaving or the withdrawal of a pupil's access.
- At both Key Stage 1 and 2, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Parents will be informed that pupils will be provided with supervised Internet access (a letter for West Hill Primary School is included as an appendix).
- Parents will be asked to sign and return a consent form. Please see the sample form later in this document.

Assessing the Risks.

West Hill Primary School Policy Statements:

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. 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 DCC can accept liability for the material accessed, or any consequences of Internet access.
- The School is aware that 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 Internet policy is implemented and compliance with the policy monitored.

Managing our Filtering System.

West Hill Primary School Policy Statements:

- The school will work in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing Subject Leader, and a record made in the Online Safety Log.
- Senior 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 Internet Watch Foundation (please see references given later).
- Filtering strategies will be selected by the school in discussion with the filtering provider where appropriate. Where possible, the filtering strategy will be selected to suit the age and curriculum requirements of the pupil. At West Hill Primary School we use the Devon countywide SWGfL filter system.

Introducing the Policy to Pupils.

West Hill Primary School Policy Statements:

- Teachers will remind the children of the policy at the start of each academic year. The children will sign the document to show they have understood the rules of Acceptable Use.
- Rules for Internet access will be posted near all computer systems.
- Pupils will be informed that Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- A module on responsible Internet use will be included in the PSHE programme covering both school and home use.

Consulting Staff.

West Hill Primary School Policy Statements:

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the School Internet 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.
- The monitoring of Internet use is a sensitive matter. Staff who operate monitoring procedures should be supervised by senior management.
- Staff development in the safe and responsible Internet use, and on school Internet policy will be provided as required.

Maintaining the ICT system security.

West Hill Primary School Policy Statements:

- The school Computing systems will be reviewed regularly with regard to security.
- Virus protection is installed and is updated regularly.
- Security strategies will be discussed with the LA, particularly where a wide area network connection is being planned.
 - Personal data sent over the Internet will be encrypted or otherwise secured.
 - Use of memory sticks will be reviewed. Personal memory sticks may not be brought into school without specific permission and a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network will be regularly checked.
 - The Computing Subject Leader / network manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

Handling complaints regarding Internet use.

West Hill Primary School Policy Statements:

- Responsibility for handling incidents is delegated to 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.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.
 - Sanctions available include:
 - interview/counselling by head of Computing and Headteacher;
 - informing parents or carers;
 - removal of Internet or computer access for a period, which could prevent access to school work held on the system, including examination coursework.

Enlisting the support of parents.

West Hill Primary School Policy Statements:

- Parents' attention will be drawn to the School Internet Policy in newsletters, the school brochure and on the school Web site.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- A stock of relevant leaflets from organisations, such as SWGfl and NSPCC, will be maintained.

Internet use across the community.

West Hill Primary School will adopt these rules as and when community use of our Computing Suite begins:

- Adult users will need to sign the acceptable use policy.
- Parents/carers of children under 18 years of age will generally be required to sign an acceptable use policy on behalf of the child.
- In libraries, children under 8 years of age must be accompanied by an adult when accessing the Internet.

This Policy should be read in conjunction with the following policies for West Hill Primary School:

West Hill Primary School	Safeguarding and Child Protection Policy
West Hill Primary School	Acceptable Behaviour Policy
West Hill Primary School	Acceptable use of Photographic Images
West Hill Primary School	Data Protection Policy and Information Sharing
West Hill Primary School	Publication Scheme
West Hill Primary School	Policy on Mobile Phones in School

Appendices:

West Hill Primary School

Foundation / KS1 Acceptable Use Policy Agreement

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):.....

Signed (teacher): **Date:**

Please Sign annually once revisited each September:

Pupil _____

Teacher _____ Date: _____

Pupil _____

Teacher _____ Date: _____

Copyright of the SWGfL School Online safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in November 2013. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal / professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

West Hill Primary School

KS2 Acceptable Use Policy Agreement

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools 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.

This Acceptable Use Policy is 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.

Acceptable Use Policy Agreement

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 username and password safe and secure – I will not share it, 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 I arrange to meet people off-line that I have communicated with on-line, 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 (eg YouTube), unless I have permission of a member of staff to do so.

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 post any school work or photographs taken in school on social media sites
- 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 from a teacher. 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 when I have permission and am supervised by a teacher.

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 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 systems and devices.

Pupil Acceptable Use Agreement Form

This form relates to the student 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 will not post any school work or photographs taken in school on social media sites
- I use my own devices in the school (when allowed) eg 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
eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil

Signature

Date

Teacher Countersignature

Please Sign annually once revisited each September:

Pupil _____

Teacher _____ Date: _____

Pupil _____

Teacher _____ Date: _____

Pupil _____

Teacher _____ Date: _____

Copyright of the SWGfL School Online safety Policy Templates is held by SWGfL. Schools and other educational institutions are permitted free use of the templates. Any person or organisation wishing to use the document for other purposes should seek consent from SWGfL and acknowledge its use.

Every reasonable effort has been made to ensure that the information included in this template is accurate, as at the date of publication in November 2013. However, SWGfL cannot guarantee its accuracy, nor can it accept liability in respect of the use of the material whether in whole or in part and whether modified or not. Suitable legal / professional advice should be sought if any difficulty arises in respect of any aspect of this new legislation or generally to do with school conduct or discipline.

West Hill Primary School Staff and Volunteer Acceptable Use Policy Agreement .

School Policy

This Policy has 'Safeguarding Children and Child Protection', the sentiments of 'Every Child Matters', 'Excellence and Enjoyment', the school's 'Healthy School', 'Eco School and Sustainable School', 'Artsmark Gold' and 'Investors in People Gold' ethos, and the school's Mission Statement and Aims at its heart.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications 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. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

This Policy should be read in conjunction with the school's Policy for 'Safeguarding Children and Child Protection.'

Acceptable Use Policy Agreement

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. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

WEST HILL PRIMARY SCHOOL
SCHOOL INTERNET POLICY AND CODE OF CONDUCT
April 2017

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. Staff should be aware that there are risks to their personal status if they use their personal email addresses or mobile phones for such communications.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use (for example: I will not take photographs of pupils / staff / parents using my mobile phone) I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on to communicate with parents / pupils.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not 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 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 install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies and I have permission to do so from the Senior Leadership Team.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will 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 download or distribute copies (including music and videos)

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

WEST HILL PRIMARY SCHOOL
SCHOOL ONLINE SAFETY POLICY and INTERNET CODE OF CONDUCT
April 2017

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Copyright of the SWGfL School Online safety Policy Templates is held by SWGfL. Every effort has been made to ensure that the information included in this template is accurate, as at the date of publication in January 2009. However, SWGfL can not guarantee it's accuracy, nor can it accept liability in respect of the use of the material.





Dear Parent/Guardian,

Use of the Internet/e-mail with classroom computers

At West Hill Primary School, we have a very successful computer system. As part of our school curriculum, your child will, at appropriate times, be given access to the Internet as an information source, communications tool and a publishing medium.

The Internet is a major source of educationally useful material and the primary distribution medium for a wide range of organisations. The potential to support the classroom teacher and the learner is significant and will continue to grow.

When using the Internet and e-mail certain conditions will apply. The purpose of these conditions is to prevent access to what might be considered offensive material or comment. Whilst it is impossible to ensure that a child will not access such material, the school, in liaison with Devon Local Education Authority, takes all reasonable steps to minimise the children's access to unsuitable material. These include:

- Use of an Internet provider that filters this type of site and enables the children to carry out searches and explore lines of enquiry more easily.
- Wherever possible all Internet access during school hours will be supervised by a member of staff or other responsible adult
- Tracking mechanisms on our fileserver system that enable the school to identify which Internet sites have been visited and to monitor Internet access
- Education of children, particularly the older children, as to the potential legal consequences of accessing certain types of material.

However, the school cannot guarantee that all such material will be blocked and for these reasons we require that you sign an Internet/e-mail user agreement which can be found attached to this letter. All users of school computer equipment are expected to use the Internet ONLY for specific activities in school as directed by the class teachers and they are expected to follow our 'Code of Conduct and Rules for Internet Use', a copy of which is attached herewith. Users not abiding by this may have their right to use the systems withdrawn, and for some offences outside authorities may have to be informed. The children are expected to use the Internet in a responsible manner and take responsibility for their actions in relation to its use. We would, therefore, ask that you be kind enough to go through the 'Code of Conduct' with your child – the amount of detail you discuss will naturally match the age and ability of each child. Each class teacher will also be discussing the Code of Conduct during lesson time. The Code will be displayed in the computer suite area and next to each class computer.

We would like to display as much information about the school as possible on our school website, which may include photographs of class groups. We shall, of course, ensure that these photographs are taken in such a way that individual children cannot be easily distinguished and **no children will be named on photographs**. Pictures may be taken of the children working at their desks or computers, or playing games in the playground or on the field. We would also like to put some of the children's work on our website in the future. We would, therefore, ask that you be kind enough to indicate on the attached form your willingness for any reference to your child to be placed anywhere on the Internet.

I should like to thank you in advance for your co-operation in this matter.

Yours sincerely,

Mrs. C. Boulton
Headteacher

Alternative Internet Use Letter

Dear Parents

Responsible Internet Use

As part of your child's curriculum and the development of Computing skills, West Hill Primary School is providing supervised access to the Internet. We believe that the use of the World Wide Web and e-mail is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Code of Conduct and Rules for Responsible Internet Use, and sign and return the consent form so that your child may use Internet at school.

Although there have been concerns about pupils having access to undesirable materials, we are taking positive steps to deal with this risk in school. Our school Internet provider operates a filtering system that restricts access to inappropriate materials. This may not be the case at home and we can provide references to information on safe Internet access if you wish.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Should you wish to discuss any aspect of Internet use please telephone me to arrange an appointment.

Yours sincerely

Mrs. C. Boulton
Headteacher

Use of the Internet Consent Form

West Hill Primary School Responsible Internet Use

Please complete, sign and return to the school secretary

Pupil:

Class:

Pupil's Agreement

I have read and understand the school Code of Conduct and Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.

Signed:

Date:

Parent's Consent for Internet Access

I have read and understood the school Code of Conduct and Rules for Responsible Internet Use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or 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:

Parent's Consent for Web Publication of Work and Photographs

I agree that, if selected, my son/daughter's work may be published on the school Web site. I also agree that photographs that include my son/daughter may be published subject to the school rules that photographs will not clearly identify individuals and that full names will not be used.

Signed:

Date:

References

Particularly for Parents

National Action for Children (NCH)

Parents Guide on Internet usage

www.nchafc.org.uk/itok/itokhome.html

Current activities to promote safe use

www.nchafc.org.uk/internet

Insafe - online safety Kit

<http://www.saferinternet.org/>

Internet Watch Foundation - report inappropriate Web sites

www.iwf.org.uk

Safe Surfing Guide for parents and carers:

www.internetwatch.org.uk/safe/index.htm

Which article on Internet filtering for home use www.internetwatch.org.uk/safe/which/total.htm

Parents Information Network (PIN)

www.pin.org.uk

Comprehensive guidelines on Internet safety

Recreational Software Advisory Council (RSACi)

www.rsac.org/

Promotes rating systems for Web sites, and is a third party rating bureau

Particularly for Schools

Associations of Co-ordinators of IT (ACITT) <http://atschool.eduweb.co.uk/acitt/aup.html>

Acceptable use policy for the Internet in UK Schools

British Computer Society

www.bcs.org.uk/iap.html

A guide for schools prepared by the BCS Schools Committee

and the National Association of Advisers for Computer Education (NAACE)

DfES Superhighway Safety

<http://safety.ngfl.gov.uk>

Essential reading. For free pack telephone: 0845 6022260

Devon Swgfl

<http://www.swgfl.org.uk/>

Internet Watch Foundation -

www.iwf.org.uk

Invites users to report illegal Web sites

Kent NGfL Initiative

www.kented.org.uk/ngfl/

Curriculum material for schools including this Internet Policy

Kent Web Skills Project

www.kented.org.uk/ngfl/webskills/

A Web site which discusses the research process and how the Web is best used in projects.

Scottish Education Department

www.scotland.gov.uk/clickthinking

Comprehensive safety advice

SEGfL ICT Security Policy

www.segfl.org.uk/

An overview of the security of networks with Internet access.

Copyright

www.templetons.com/brad/copymyths.html

Covers the main aspects of copyright of digital materials, US-based but relevant.

Internet Users Guide

www.terena.nl/libr/gnrt/

A guide to network resource tools, a book (ISBN 0-201-61905-9) or free on the Web.

Notes on the legal framework

West Hill Primary Schools is aware of the following legislation that may be relevant.

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, data theft or to damage the system or data. The Rules for Responsible Internet Use remind users of the ownership of the school computer system.

Monitoring of data on a school network 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 interests 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 a school's computer system, but then allow private use following application to the head teacher. The Rules for Responsible Internet Use, which every user must agree to, contain 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.

The following legislation is also relevant:

Data Protection Act 1984/98 concerns data on individual people held on computer files and its use and protection.

Copyright, Design and Patents Act 1988 makes it an offence to use unlicensed software

The Telecommunications Act 1984 Section 43 makes it an offence to send offensive or indecent materials over the public telecommunications system.

Protection of Children Act 1978

Obscene Publications Act 1959 and 1964 defines "obscene" and related offences.

References:

Brief introduction to dangers and legal aspects of the Internet.

www.bbc.co.uk/webwise/basics/user_01.shtml

List of useful law resources; see copyright and Internet sections.

<http://link.bubl.ac.uk/law>

HMSO: Full text of all UK legislation and purchase of paper copies.

www.legislation.hms.gov.uk