# Online Safety Policy

# Wheelwright Lane Primary School

Date written: December 2015
Review: December 2016

## Online Safety Policy

Wheelwright Lane takes the safety of all children and adults very seriously. This policy is written to protect all children and adults within the school.

We recognise that online safety encompasses not only Internet technologies, but also electronic communications such as mobile phones, tablets and wireless technology. It highlights the need to educate pupils about the benefits it can have to broaden their learning experiences and develop creativity in and out of school. However, it is also important to consider the risks associated with using this technology, providing users with safeguards and awareness for them to enable and control their online experience.

Internet use and online safety is part of the statutory National Curriculum and is a necessary tool for staff and pupils. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning.

Wheelwright Lane's online safety policy operates in conjunction with other policies including those for Behaviour, Anti-Bullying, Curriculum, Data Protection, Safeguarding, Health and Safety and Security.

## End to End Online Safety

Online Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff, pupils, governors and volunteers; supported by regular updates from IT subject leader and senior leaders and made explicit through published policies.
- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from the Warwickshire Broadband including the effective management of Websense filtering and Policy Central monitoring.
- National Education Network standards and specifications.
- E-Cadets monitor Apps, games and online usage of pupils within the school. Their findings will inform the Online Safety coordinator, who will research whether they are safe for children to use. Pupils and parents are then informed via the school newsletter, assemblies, website and online safety lessons as to their safe use.
- Online safety assemblies are carried out termly to remind children how to keep themselves safe online and report any concerns they have.

## 1.1 Writing and reviewing the online safety policy

The Online Safety Policy is an integral part of the curriculum and relates to other policies including those for Safeguarding and for Child Protection.

- The school has appointed an Online Safety Coordinator (Mrs Hammonds) and the Designated Safeguarding Lead is the Headteacher (Mrs Browne) Both are responsible for overseeing the online safety of children.
- Our Online Safety Policy has been written by the school, building on the Warwickshire ICT Development Service Online Safety Policy and government guidance. It has been agreed by the senior management, all staff and approved by governors.
- The Online Safety Policy will be reviewed annually.

## 1.2 Teaching and learning

### 1.2.1 Why Internet use is important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use and online safety is a part of the statutory curriculum and a necessary tool for staff and pupils.

### 1.2.3 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 (Warwickshire firewall).
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils. However, unsupervised access to the internet is not permitted.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

### 1.2.4 Pupils will be taught how to evaluate Internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to Warwickshire ICT Development Service, and where appropriate the school online safety leader (IT subject leader or IT technician).
- Schools should ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught how to report suspicious activity and abuse online through online safety lessons and assemblies as part of the Computing curriculum.
- Posters are located in classrooms and Computing suite to remind children what to do if they come across suspicious activity or abuse online.

## 1.3 Managing Internet Access

### 1.3.1 Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses the Warwickshire Broadband with its firewall and filters.
- The school provides an addition level of protection through its deployment of Policy Central in partnership with Warwickshire ICT Development Services.

### 1.3.2 E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Use of words included in the Policy Central 'banned' list will be detected and logged.
- Whole-class or group e-mail addresses can also be used.
- 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 spam mail is not permitted.

### 1.3.3 Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

### 1.3.4 Publishing pupil's images and work

- Only photographs of children with parental permission will be published on the website.
- Pupils' full names will not be used anywhere on the Web site, the school will only use the child's first name.
- Written permission from parents or carers will be obtained in Nursery/Reception or in new starter packs before photographs of pupils are published on the school Web site.
- Pupil's work can only be published with the permission of the pupil and parents.

### 1.3.5 Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind or include photographs of them in school uniform which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.
- Pupils are advised by staff of sites which are safe for them to use with friends and content they should include online e.g. photographs, usernames, personal information.
- Staff and parents are given advice (see Complaints policy) explaining expectations for appropriate online behaviour and expected to sign a social network agreement.

### 1.3.6 Managing filtering

- The school will work in partnership with the Warwickshire ICT Development Service and Becta to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the school Online-Safety coordinator or Computing technician (K. Frith).
- Senior staff will ensure that regular discussions with staff and checks are in place to ensure that the filtering methods selected are appropriate, effective and reasonable.

### 1.3.7 Managing videoconferencing

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- External IP addresses should not be made available to other sites.
- Pupils are supervised by a teacher before making or answering a videoconference call.
- Video conferencing should be supervised appropriately for the pupils' age.

### 1.3.8 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.
- Pupils are only permitted to have mobile phones in school with the head teacher's permission. Children granted permission are to hand mobile phones into the school office at the start of the school day, to be locked away by the school secretary and collected at the end of the day when leaving the school grounds.
- Staff, volunteers and other adults working in the school will keep mobile phones in a secure place, usage is not permitted during lessons. (See Code of Conduct).
- Staff will be issued with a school phone where contact with pupils or parents (Manor Adventure Trip) is required.

### 1.3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Pupils, staff, parents, governors and other adults working in school will be advised on how to protect personal data online.

## 1.4 Policy Decisions

### 1.4.1 Authorising Internet access

- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff and pupils must read and sign the acceptable ICT use agreement, 'Online Safety Agreement Form for School Staff', before using any school ICT resource. (See Appendix 2)
- At Early Years and Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.

- At Key Stage 2 children are allowed to access the internet during lesson and Golden Time when supervised by an adult.
- All parents, pupils, governors and other staff will be asked to sign and return a consent form (Appendix 2).

#### 1.4.2 Assessing risks

- 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 WCC can accept liability for the material accessed, or any consequences of Internet access.
- The head teacher will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.

#### 1.4.3 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 child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Procedures within the school behaviour policy include:
  – interview/counselling by phase leader/class teacher;
  – informing parents or carers;
  – removal of Internet or computer access for a period.

#### 1.4.4 Community use of the Internet

- The school will liaise with local organisations including the Bedworth Consortium to establish a common approach to online safety.
- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- Online safety coordinator and E Cadets will continue to liaise with pupils and provide support when children have concerns.

## 1.5 Communications Policy

#### 1.5.1 Introducing the e-safety policy to pupils

- Rules for Internet access will be posted in all networked rooms and classrooms.
- Pupils will be informed that Internet use will be monitored.
- An Online Safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use as part of the Computing curriculum.

### 1.5.2 Staff and the Online Safety policy

- 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. Discretion and professional conduct is essential.
- Staff are to address online safety within their computing lessons to raise awareness and remind children how to use different devices safely.
- Staff will sign an internet and social media agreement informing them of what is deemed as acceptable behaviour for them to abide by.

### 1.5.3 Enlisting parents' support

- On the school Web site parents' attention will be drawn to the School Online Safety Policy in newsletters and the school brochure.
- Online safety advice is published on the school newsletter regularly to inform parents of new advice available and any new APPS or games which have been found to be unsafe for children to use.
- Online safety evenings have been offered to parents and information been made available on Parents' evenings.
- Parents are encouraged to liaise with the school if they suspect, or have identified, that their child is conducting risky behaviour online, as well as being a victim of abuse or inappropriate behaviour from others when online.

This policy was agreed by staff on_____11th December 2015_____
This policy was presented to Governors on _3rd March 2016 and ratified on that date. This will be reviewed annually.
Signed……

**Appendix 1: Internet use - Possible teaching and learning activities**

| Activities | Key e-safety issues | Relevant websites |
|---|---|---|
| Creating web directories to provide easy access to suitable websites. | Parental consent should be sought.<br><br>Pupils should be supervised.<br><br>Pupils should be directed to specific, approved on-line materials. | Web directories e.g.<br>Google |
| Using search engines to access information from a range of websites. | Parental consent should be sought.<br><br>Pupils should be supervised.<br><br>Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with. | Web quests e.g.<br>Ask Jeeves for kids<br>Yahooligans<br>CBBC Search<br>Kidsclick<br>Picsearch<br>safesearch |
| Exchanging information with other pupils and asking questions of experts via e-mail. | Pupils should only use approved e-mail accounts.<br><br>Pupils should never give out personal information.<br><br>Consider using systems that provide online moderation e.g. SuperClubs. | RM Easimail<br>Kids Safe Mail<br>E-mail a children's author<br>E-mail Museums and Galleries |
| Publishing pupils' work on school and other websites. | Pupil and parental consent should be sought prior to publication.<br><br>Pupils' full names and other personal information should be omitted. | School website<br>Purple Mash |
| Publishing images including photographs of pupils. | Parental consent for publication of photographs should be sought.<br><br>Photographs should not enable individual pupils to be identified.<br><br>File names should not refer to the pupil by name. | School website |
| Communicating ideas within chat rooms or online forums. | Only chat rooms dedicated to educational use and that are moderated should be used.<br><br>Access to other social networking sites should be blocked.<br><br>Pupils should never give out personal information. | SuperClubs<br>Skype<br>FlashMeeting |
| Audio and video conferencing to gather information and share pupils' work. | Pupils should be supervised.<br><br>Only sites that are secure and need to be accessed using an e-mail address or protected password should be used. | Skype<br>National Archives "On-Line"<br>Global Leap<br>National History Museum<br>Imperial War Museum |

## Appendix 2: Acceptable use policies

### Acceptable Use Policy (I. T.) for Learners in KS1

***I want to feel safe all the time.***

I …… agree that I will:

- only keep the details of my passwords with adults in school and at home with my parents
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email in school
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home, school, family, friends and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

I have had this read to me and understand how (or know who to ask for help) to use the computers at school.

Pupils Name…….  Parents signature…….

Class…….  Pupils signature…….

Date…….

## *Acceptable Use Policy ( I. T.) for learners in KS2*

*When I am using the computer or other technologies, I want to feel safe all the time.*

I …….agree that I will:

- In year 5 and 6 always keep details of my passwords secret and in year 3 and 4 only give this information to my parents or approved adults in school.
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved and deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not have my own mobile device in school
- only give my mobile phone number to friends I know in real life and trust
- only email people I know or have been approved by my school
- in school only use email application which has been provided by school
- discuss and agree my use of a social networking site with a responsible adult before joining (facebook users have to be over 14yrs old)
- always follow the terms and conditions when using a site
- always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me

*I know that anything I share online may be monitored. I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.*

I have read this/had this read to me and understand how to use the computers at school.

Pupils Name……. Parents signature…….

Class…… Pupils signature…….

Date……

## Acceptable Use Policy (I.T.) for Governors

***The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to support learning without creating unnecessary risk to users.***

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school, building on the WMnet e Safety guidance and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology (using the Self-Review Framework) to establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

I have read this and understand how to use the computers in school.

Governors Name……. E-safety governors name…….

Signature…….

Signature…….

Date…….
Date……..

***Acceptable Use Policy (I.T.) for adults working with learners in school.***

***The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.***

I agree that I will:

- only use, move and share school data securely
- respect the school network security. All removable devices used in school to be encrypted and checked for viruses before files are opened.
- implement the schools policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- only give permission to pupils to communicate online with trusted users.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils or parents
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the named e-Safety officer
- promote any supplied E safety guidance appropriately.

***I know that anything I share online may be monitored.***

***I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.***

I agree that I will not:

visit Internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- pornography (including child pornography)
- promoting discrimination of any kind
- promoting violence or bullying
- promoting racial or religious hatred
- promoting illegal acts
- breach any Local Authority/School policies, e.g. gambling
- do anything which exposes others to danger
- any other information which may be offensive to others
- forward chain letters
- breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission and information subsequently to be deleted as soon as possible.

- store images or other files off site without permission from the head teacher or their delegated representative
- store personal information, together with school content on any removable devices that I bring into school
- retain personal information on school equipment  eg. Laptops, video recorders.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential.  The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

***I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.***

I have read this and understand how to use I.T. in school

Adult/Staff Name…… Authorised by……..

Signature……
Signature…….

Date…….
Date…….