Whitnash Primary School

‘Learning, growing and succeeding together’

Online Safety Policy

The school's Online Safety Co-ordinator is:

Mr David Hitchins

hitchins.d@welearn365.com

The school's Online Safety Governors is:

Wai-Hong Lee

waihonglee1@gmail.com

The following members of our team have the overall editorial responsibility for the school website, Facebook and communications:

Miss Jackie Hall (office Manager and PA to the Head)

Hall.j3@welearn365.com

Mrs Donna Ellison (Headteacher)

Ellison.d@welearn365.com

Mr David Hitchins

hitchins.d@welearn365.com

School Online Safety Policy

The writing and reviewing the Online Safety Policy:

- The Online Safety Policy relates to other policies including those for Computing and for child protection.
- The school has appointed an Online Safety Officer, a Link Governor for ICT and a Link Governor for Safeguarding.
- Our Online Safety Policy has been agreed by the Senior Management Team and approved by Governors.
- The Online Safety Policy will be reviewed every year.

Teaching and learning

Why Internet use is important?

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

Internet use will enhance learning

- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils by Firewall Filtering and Safe Guarding Package from WES.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities.
- Staff 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.

Aims and Objectives

- To provide staff with the key information to deal with online safety issues in a safe and effective manner.
- To ensure that staff have the ability to deal with content, contact and conduct issues on line.
- To provide staff with a point of reference when dealing with online safety issues.
-

Equal Opportunities

- All children should have equal access to the use of the Internet.
- Further information on equal opportunities and special needs is given in the relevant school policies.

Organisation

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, (e.g. using search engines) staff should be vigilant in monitoring the content of the websites the pupils visit and provide close supervision.
- 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

- KS1 - Pupils should be taught to: use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- KS2 - Pupils should be taught to: use technology safely, respectfully and responsibly; recognise acceptable/ unacceptable behaviour; identify a range of ways to report concerns about content and contact.
- The school has an Online Safety Committee of children who look at making improvements and raise awareness of Online Safety.

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 the Online Safety Officer, who then must report it to Warwickshire ICT Development Service. Tel: 414100
- The school will ensure 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.

Managing Internet Access

Information System Security

- The security of the school information systems will be reviewed regularly.
- Virus protection is installed and updated regularly by Launch Systems.
- The school uses the Warwickshire Broadband with its firewall and filters.
- The school provides an additional level of protection through its deployment of Warwickshire ICT Development Service monitored system called ‘Policy Central’. This software monitors text appearing on the screen and keyboard input, identifying the use of words that are included on a list of ‘banned words’. The software captures the screen, identifying machine and user details so appropriate action can be taken.

E-mail

Pupils currently do not use e-mail accounts on the school system.

Passwords

All users will be provided with a username (and KS2 password)

The “master / administrator” passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place.

Publishing

Published content and the school website

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The Headteacher and Lead Office Manager will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The school does not permit the use of social media, or web based communication platforms, such as a website by any other volunteer organisation under the umbrella of Whitnash Primary School without the express permission of the Governing Body.
- The content of communication via the school website or the school's social media for volunteer organisations under the umbrella of Whitnash Primary School require the full approval of the Headteacher and Lead Office Manager with editorial responsibility for these communication platforms. This is necessary to ensure that content is accurate and appropriate.

Publishing pupils' images

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be identified by name.
- Written permission from parents or carers will be obtained before photos of pupils will be used for display and educational use, the portal, publications, on the school website by us, by the Local Authority or by local newspapers.
- The content of communication via the school website, the school's social media or advertisement letters and fliers for volunteer organisations under the umbrella of Whitnash Primary School, also need to ensure full permission has been given for pupils images to be used for such communications.
- The Headteacher and Lead Office Manager has overall editorial responsibility and ensure that content is accurate and appropriate, and must therefore be consulted by such organisations.

Publishing pupils' names

- Recordings that are published will only use pupils' first names.

Social networking and personal publishing

- Social networking sites, chat rooms and newsgroups are not permitted without the express permission from the school's Governing Body.
- Publishing on the school Face Book account is only permitted by staff with permitted editorial responsibility, following strict procedures.

- Pupils and parents are advised that the use of social network spaces outside school may be inappropriate for pupils.

- Pupils are advised never to reveal personal details of any kind 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.

Managing filtering

- The school will work in partnership with the Warwickshire ICT Development Service to ensure filtering systems are as effective as possible.

- The Online Safety Officer will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the new General Data Protection Regulation Guidance May 2018.

Handling Online Safety complaints

- Any complaints of Internet misuse are dealt with initially by the Online Safety Officer and/or Headteacher.

- Any complaint about staff misuse must be referred to the Headteacher.

- Any complaint about parent/community misuse must be referred to the Headteacher.
- Any complaint about the Headteacher must be referred to the Chair of Governors.
- Any complaints of a child protection nature will be dealt with in accordance with school child protection procedures.

Community use of the Internet

- The school is sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- Wider community use will fall under the same obligations as the staff use.

Communications

Introducing the Online Safety Policy to pupils

- The Online Safety Pupil Committee meet each half-term.
- Rules for responsible ICT use are posted in all networked rooms.
- Pupils are informed that Internet use will be monitored.
- The school participates in the annual E-Safety Awareness Week

- Regular Online Safety training will be provided to raise the awareness and importance of safe and responsible Internet use.

Staff and the Online Safety Policy

- All staff are given the School Online Safety Policy and its importance explained.
- All staff and volunteers read and sign the School Online Safety Agreement Form each September.
- Staff are made aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- All staff are made aware of the reference made to Online Safety in the Staff Code of Conduct.

Enlisting parents' support

- Parents' attention will be drawn to the School Online Safety Policy in newsletters and on the school web site.
- The need for a parents meeting or information leaflet will be reviewed annually
- Wider guidance of Online Safety is provided through the school website, Newsletter and Face Book
- The school conducts Online Safety Questionnaires with parents to guide the content of this guidance

Monitoring

Authorising Internet access:

- The school maintains a current record of all staff and pupils who are granted Internet access in the WI-FI Agreement File kept in the School Office.
- All staff must read and sign the acceptable ICT use agreement, 'Online Safety Agreement Form for School Staff', before using any school ICT resource.
- Parents are requested to sign the 'Online Safety Agreement' form for parents of Primary aged children' as part of the Home/School Agreement.
- Children sign the 'Online Safety Agreement' form for KS1 / KS2 school pupils.

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 Online Safety Officer will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Recording reported events.
- The Headteacher ensures that the Online Safety Policy is implemented and compliance with the policy is monitored.

Education

Pupils:

- Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's Online Safety provision. Children need the help and support of the school to recognise and avoid online safety risks and build their resilience.
- Online Safety education will be provided through the Computing schemes of work in the following ways:

✓ A planned Online Safety programme should be provided as part of Computing / PHSE / 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 PSHE 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 should be encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school

✓ Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet

✓ Staff should act as good role models in their use of ICT, the internet and mobile devices

Parents/carers:

- Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, website

- Online safety parent sessions as required
- 1-2-1 parent/carer meetings

Education- extended schools

On occasion the school may offer family learning courses in online safety so that parents and children can together gain a better understanding of these issues. Messages to the public around online safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

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.
- 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 Officer (or other nominated person) will receive regular updates through attendance at LA / other information / training sessions and by reviewing guidance documents released by BECTA / 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 Officer will provide advice / guidance / training as required to individuals as required

Training - governors

- Governors should take part in online safety training / awareness sessions when available, with particular importance for those who are members of any sub-committee / group involved in ICT / online safety / health and safety / child protection.

This may be offered in a number of ways:

- ✓ Attendance at training provided by the Local Authority / National Governors Association or other relevant organisation.
- ✓ Participation in school training / information sessions for staff or parents

Communications

Communication technologies:

A wide range of rapidly developing communications technologies has the potential to enhance learning. The school currently considers the benefit of using these technologies for education and considers it the benefits of their use in school outweighs their risks / disadvantages.

Currently the school currently allows pupils to bring their mobile phones to school, for safety reasons, but insist that these are kept in the school office until home time.

The school, at times, permits the use of Blogs and Email where their use is linked to curriculum activities/learning.

The school does not permit the use of Social Networking, Chat Rooms or Instant Messaging.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored.
- Users need to be aware that email communications may be monitored
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official school email address should be used by parents/carers to communicate with staff members

Responding to Incident of Misuse

Illegal activity:

- It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:
- Examples of illegal activity could include:
- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials

Inappropriate activity:

- It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures. Inappropriate use may result in a referral to the Online Safety Officer Refer, the Headteacher or to the Police.
- Sanctions for misuse may include, informing parents / carers, the removal of network / internet access rights, Warnings, Consideration of further sanction e.g. detention / exclusion.

- *Examples of misuse are as follows:*
  - accessing or trying to access material that could be considered illegal
  - Unauthorised use of non-educational sites during lessons
  - Unauthorised use of mobile phone / digital camera / other handheld device
  - Unauthorised use of social networking / instant messaging / personal email
  - Unauthorised downloading or uploading of file
  - Allowing others to access school network by sharing username and passwords
  - Attempting to access or accessing the school network, using another student's / pupil's account
  - Attempting to access or accessing the school network, using the account of a member of staff
  - Corrupting or destroying the data of other users
  - Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
  - Continued infringements of the above, following previous warnings or sanctions
  - Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
  - Using proxy sites or other means to subvert the school's filtering system
  - Accidentally accessing offensive or pornographic material and failing to report the incident
  - Deliberately accessing or trying to access offensive or pornographic material
  - Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

Staff inappropriate activity:

Examples of misuse are as follows:

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
- Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
- Careless use of personal data eg holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature
- Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the school's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Breaching copyright or licensing regulations
- Continued infringements of the above, following previous warnings or sanctions

Sanctions for staff misuse may include:

- Refer to Online Safety Officer
- Refer to Headteacher
- Refer to Local Authority / HR / LADO
- Refer to Police
- Refer to Technical Support Staff for action re filtering etc
- Warning Suspension
- Disciplinary action

Developments

Managing emerging technologies:

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

- Mobile phone technology will not be used during lessons or formal school time by pupils – see separate mobile phone policy and Staff Code of Conduct Policy.
- Staff must not use their own mobile phone where contact with parents/carers is required. The school office shall be used as the primary point of contact, if off-site.

Date of Policy: Summer 2018

Policy Review date: Summer 2019

Online Safety Agreement Form
For School Staff

- I understand that the network is the property of the school and agree that my use of this network must be compatible with my professional role.
- I understand that the school ICT systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that use for personal financial gain, gambling, political purposes or advertising is not permitted.
- I understand and agree that the school will monitor my network and Internet use to ensure policy compliance.
- I will respect ICT system security and understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will not install any software or hardware without permission.
- I will not disclose any password or login name to anyone, other than, where appropriate, the staff responsible for maintaining the system.
- I will take all reasonable precautions to secure data or equipment taken off the school premises.
- I will report any incidents of concern to the school's Designated Child Protection Staff or Online Safety Officer as appropriate.
- I will ensure that my electronic communications with pupils are compatible with my professional role and cannot be reasonably misinterpreted.
- I will promote online safety with the pupils that I work with and will help them to develop a responsible attitude to ICT use.
- I will respect copyright and intellectual property rights.

The school will exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed: …….. Capitals: ……
Accepted for School: ……. Capitals: …….
Date: ……..
This form is valid for the time the staff member is employed at the school and will automatically expire after this time.

Online Safety Agreement Form
For Community Use

- I understand that the network is the property of the school and agree that my use of this network must be compatible with an agreed community use.
- I understand that the school ICT systems may not be used for private purposes, without specific permission from the Headteacher.
- I understand that use for personal financial gain, gambling, political purposes or advertising is not permitted.
- I understand and agree that the school will monitor my network and Internet use to ensure policy compliance.
- I will respect ICT system security and understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will not install any software or hardware without permission.
- I will not disclose any password or login name to anyone, other than, where appropriate, the staff responsible for maintaining the system.
- I will take all reasonable precautions to secure data or equipment taken off the school premises.
- I will report any incidents of concern to the school's Designated Child Protection Staff or Online Safety Officer as appropriate.
- I will respect copyright and intellectual property rights.

The school will exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Signed: …….…. Capitals: …….
Accepted for School: ……. Capitals: …….
Date: ……..

This form is valid for the period of agreed usage.

Safety Agreement Form
For Parents of Key Stage 2 Aged Children

Parent / guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter / son to have access to use the Internet and other ICT facilities at school.

I know that my daughter / son has signed an online safety agreement form and that they have a copy of the “12 Rules for responsible ICT use”.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using an educationally filtered and monitored service, employing appropriate teaching practice and teaching online safety skills to pupils.

I understand that the school can check my child’s computer files, and the Internet sites they visit, and that if they have concerns about their online safety or online behaviour that they will contact me.

I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child’s online safety.

Parent / guardian signature: _____
Date: ___/___/___

This form is valid for the period of the time your child attends this school and will automatically expire after this time. 19

Online Safety Agreement Form

For Primary School Pupils – Key Stage 2

Keeping Safe:
Stop, Think, Before you click!

Pupil name: _____

I have read the school's '12 Rules for responsible ICT use'. My teacher has explained them to me.

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules.

This means I will use the computers, Internet, online communities, digital cameras, iPads, video recorders, and other ICT in a safe and responsible way. I understand that the school can check my computer files, and the Internet sites I visit, and that if they have concerns about my safety, they may contact my parent / guardian.

Pupil's signature _____

Date: ___/___/___

This form is valid for the period of the time I attend this school and will automatically expire after this time.

Online Safety Agreement Form

For Primary School Pupils – Key Stage 1

Think then Click

These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can only click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

Only use your own login

My name is : _____

Keeping Safe:

Stop, think, before you Click!

12 Rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the school's ICT equipment for schoolwork and homework.

2. I will only delete my own files.

3. I will not look at other people's files without their permission.

4. (I will keep my login and password secret.)

5. I will not bring memory/usb sticks into school without permission.

6. I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.

7. When using ICT equipment, I will always be polite and sensible.

8. I will not open an attachment, or download a file, unless I have permission.

9. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends.

10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room.

11. If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

12. I will not take photos or videos of others without permission.