

Stockton Wood Community Primary School i-Speke out!

Responsible Use Policy for e-safety

Date for review: September 2017

Terms of reference:

Child Protection Officer: Suzy Stacey

Deputy Child Protection Officer: Nicola Ware

E-Safety Co-ordinator: Nicola Ware E-Safety Governor: Richard Finch

Policy Statement:

The policy aims to raise awareness and state expectations of school staff detailing their responsibilities for monitoring of teaching about e-safety.*

*E-Safety: The responsible and safe use of any means of electronic communication.

The following stakeholders are responsible for ensuring that:

























2

School Management:

- 1. A secure, password protected system is provided for stakeholders to use.
- 2. The e-safety policy and practices are implemented and reviewed.
- 3. Technical support is in place.
- 4. A planned programme of formal e-safety training will be made available to all staff, including new staff and NQTs,

School staff:

- 1. They have an up to date awareness of e-safety matters and the current school e-safety policy and practices.
- 2. They have read, understood and signed the school staff Responsible Use Policy.
- 3. They report any suspected misuse or problem to the E-Safety co-ordinator/ Child Protection Officer/ Head teacher for investigation/action/sanction.
- 4. Digital communications with all stakeholders should be on a professional level using the school e-mail system. (Teacher Standards Appendix 1)
- E-safety issues are embedded in all aspects of the curriculum and other school activities.
- All members of the school community follow the school e-safety and Responsible use policy.
- 7. They monitor ICT activity in lessons, extra curricula and extended school activities.
- 8. They are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices. (See Appendix 2)











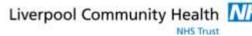














3

- 9. That learner's research skills are developed as appropriate to age and learners are guided to suitable sites.
- 10. That processes are in place for dealing with any unsuitable material that is found in internet searches.

Learners:

- Are responsible for using school ICT systems in accordance with the Learner Responsible use policy, which they will be expected to sign before being given access to school systems. (At Key Stage 1 parents/carers would be expected to sign on behalf on the learner.)
- 2. To have an age appropriate understanding of research skills (and acknowledge the source if necessary).
- 3. Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- 4. Will be expected to know and understand the school policies on mobile phones, digital cameras and handheld devices. They should know and understand the school policies on the taking/ use of images and on cyber bullying.
- 5. Should understand the importance of adopting responsible e-safety practice when using digital technologies out of school and that their actions can have an impact on school life.

Parents/ Carers and Extended School Groups

1. Parents/ carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in a responsible way. The school will

























4

- therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters and the i-Speke out website.
- Parents will be responsible for endorsing by signature the Learner Responsible Use Policy.
- 3. Extended Schools will accept and follow the school's current policy and practice further guidance will be available through the **i-Speke out!** Website.

Governors:

- 1. The Governor with responsibility for e-safety will receive training and will be aware of all current policies and practices.
- 2. They will be made aware of the number and type of e-safety incidents reported to school.

Curriculum:

- 1. E-safety will be taught through the curriculum this will cover both the use of ICT and new technologies in school and outside school.
- Key e-safety messages should be reinforced through assemblies and collective worship.
- Learners should be taught in all lessons to be critically aware of the content online and be guided in an age appropriate manner to validate the accuracy of information.

Digital Photography / Digital Video

1. When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In











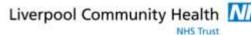














particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but
 must follow school policies concerning the sharing, distribution and publication of
 those images. Those images should only be taken on school equipment, the
 personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are
 appropriately dressed and are not participating in activities that might bring the
 individuals or the school into disrepute.
- 4. Students / pupils must not take, use, share, publish or distribute images of others without their permission
- 5. Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- 6. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.











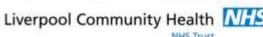














User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make,	child sexual abuse images					
to:	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					
	adult material that potentially breaches the Obscene Publications Act in the UK					
	criminally racist material in UK					
	pornography					
	promotion of any kind of discrimination					
	promotion of racial or religious hatred					
	threatening behaviour, including promotion of physical violence or mental harm					
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute					
Using school systems to run a private business						
Use systems, applications, websites or other mechanisms that by employed by SWGfL and / or the school	pass the filtering or other safeguards					
Uploading, downloading or transmitting commercial software or at third parties, without the necessary licensing permissions	ny copyrighted materials belonging to					
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)						
Creating or propagating computer viruses or other harmful files						
Carrying out sustained or instantaneous high volume network traf causes network congestion and hinders others in their use of the						
On-line gaming (educational)						

























On-line gaming (non educational)			
On-line gambling			
On-line shopping / commerce			
File sharing			
Use of social networking sites			
Video broadcasting eg Youtube			

Students / Pupils

Incidents:	Refer to class teacher	Refer to E- Safety co-ordinator	Refer to Headteacher	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction inline with school behaviour policy
Deliberately 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 files								
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				
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

Actions / Sanctions

Incidents:	Refer to line manager	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
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 e.g. 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 students / 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				
Use of personal mobile phone at time or in ways other than set out by the "Mobile Phone Policy"				

























Appendix 1 Teacher Standards – September 2012 PREAMBLE

Teachers make the education of their pupils their first concern, and are accountable for achieving the highest possible standards in work and conduct. Teachers act with honesty and integrity; have strong subject knowledge, keep their knowledge and skills as teachers up-to-date and are self-critical; forge positive professional relationships; and work with parents in the best interests of their pupils.

PART TWO: PERSONAL AND PROFESSIONAL CONDUCT

A teacher is expected to demonstrate consistently high standards of personal and professional conduct. The following statements define the behaviour and attitudes which set the required standard for conduct throughout a teacher's career.

- Teachers uphold public trust in the profession and maintain high standards of ethics and behaviour, within and outside school, by: treating pupils with dignity, building relationships rooted in mutual respect, and at all times observing proper boundaries appropriate to a teacher's professional position.
- having regard for the need to safeguard pupils' well-being, in accordance with statutory provisions showing tolerance of and respect for the rights of others.

























- not undermining fundamental British values, including democracy, the rule of law, individual liberty and mutual respect, and tolerance of those with different faiths and beliefs.
- ensuring that personal beliefs are not expressed in ways which exploit pupils'
 vulnerability or might lead them to break the law.

Appendix 2:

School data

- Do not store images and video of students on a personal device Use Schoolprovided equipment to record and store images and video taken of students.
- Student data such as full names, addresses, ethnic origin, socio-economic status,
 FFT data, etc. should never be stored on personal devices.

Use of personal equipment

 Use of personal electronic equipment owned by staff within the School should be cleared by Mrs. Stacey. Regulations for PAT testing, Viruses, data sharing and breakages may deem this unsuitable.

Network Access

 Staff can use the network for work related tasks in their own time. Accessing auction sites, banks and any other commercial site that is not related directly to the teaching and learning of the pupils is strictly prohibited.











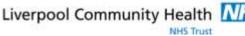














Stockton Wood Mobile Phone Policy

Audience: School Staff

Date for review: September 2017

Terms of reference:

Child Protection Officer: Suzy Stacey

Deputy Child Protection Officer: Nicola Ware

E-Safety Co-ordinator: Nicola Ware

E-Safety Governor: Richard Finch

Policy Statement:

The policy aims to state expectations of school staff, pupils, visitors and other community users regarding use of personal mobile phone devices.

Pupils:

- Children are not permitted to bring mobile phones to school.
- Parents wishing their child to carry a mobile phone for a specific purpose must obtain written permission from the Head teacher first. Permission must be granted and not assumed.
- Children found with mobile phones when permission has not been granted by the Head teacher will have their phone confiscated. (See Searching for devices prohibited by school policy)

























Staff:

- Staff are required to switch their phones off between the hours of 8.45am and 3.45pm, these should be placed and remain out of sight.
- Staff may switch on mobile phones during lunch hour and during PPA whilst in designated areas.
- Staff may only switch on mobile phones in the staff room or other room in which children do not have access or are not expected to access.
- All telephone calls between the hours of 8.45am and 3.45pm must be directed to the school switchboard.
- Staff taking children on educational visits or residential visits will be provided with a school mobile phone.
- Staff must remain vigilant to ensure the policy is upheld.

Cleaning Staff:

- Staff are required to switch their phones off during their hours of work, phones should be placed and remain out of sight.
- All telephone calls between working hours must be directed to the school switchboard.
- Staff must remain vigilant to ensure the policy is upheld.

























Visitors:

- Visitors must switch off their phones on entering the building and phones must remain switched off whilst they are on the school site and children are present.
- Visitors will be prompted to do this on entry to the school site.
- Signage will be prominently displayed reinforcing that mobile phones must be switched off.
- Visitors wishing to make a phone call will be allowed to use the school telephones as long as the call is of benefit to the school.

Community Users:

- Community users must switch of their phones on entering the building and phones must remain switched off whilst they are on the school site and children are present.
- Community users will be prompted to do this on entry to the school site.
- Community users to make a phone call will be allowed to use the school telephones as long as the call is of benefit to the school.

























Appendix 3:

Procedural Guide:

Cyber bullying incident:

- Incidents should be recorded on a school incident sheet and passed to the e-safety co-ordinator / Child Protection officer who will decide upon an appropriate course of action.
- Incident sheets should be signed and dated.

Child discovered with mobile phone:

- Phone should be confiscated by member of staff.
- Phone should be passed to the Head teacher, Deputy Head Teacher or in their absence member of Senior Management team.
- Parents to be notified by Head teacher or appropriate member of staff.

Inappropriate content discovered:

 Details of the content (including web address) should be recorded on an incident sheet and be passed to the E-Safety Co-ordinator who will block the content using the school filtering system.

























Personal Declaration:

<u> </u>		have	read	and
understood the Stockton Wood Responsible Use Policy	and	Stockton	Wood	Mobile
Phone Policy including sanctions set out:				
Signed:				
Date:				
Signed on behalf of Stockton Wood by:				_
Signature:				
Date:				





















