Whitehall Nursery and Infant School

E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband from LA ICT including the effective management of filtering.
- National Education Network standards and specifications.

School e-safety policy

- The e-safety policy relates to other policies including those for ICT, bullying and for child protection.
- E-safety coordinators:
  - For school and staff – Computing Lead
  - For parents – Parent Support Advisor
- Our e-safety policy has been agreed by senior management and approved by governors.
- The e-safety policy and its implementation will be reviewed annually.

Why Internet use is important

- The Internet is an essential element for education, business and social interaction. It has become an integral part of life. Children need to learn its potential for supporting their knowledge, development and opportunities but also understanding the limitations and potential dangers to individual and collective wellbeing. The school has a duty to provide students 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 for pupil use and includes filtering appropriate to the age of pupils.

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Key e-safety messages will be reinforced as part of a planned sequence of lessons and circle time using resources from https://www.thinkuknow.co.uk/

Managing Internet Access

- Information system security, School ICT systems, capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with LA ICT.

Published content and the school website

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

Pupil's images and work

- Pupils' full names will not be used anywhere on the school website or in newsletters particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or in newsletters.
- Pupil's work can only be published with the permission of the pupil and parents.
- If any parent wishes to withdraw their permission for images of their child to be used on the website and in newsletters they must inform the Head teacher in writing.
- Staff may use their iPads to take photographic and video evidence of children's learning.
- If iPads are to be taken home, all photos and videos of children are to be deleted.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social networks outside school is inappropriate for primary aged pupils.
- Staff will not post details of the school on any social networking sites.
- Any personal social networking accounts must be made private and staff are not permitted to communicate with any parents or pupils on these sites.

Managing filtering

- The school will work with LA ICT to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the named e-safety coordinator.
- SMT 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 Data Protection Act 1998.
- Any digital documents containing pupils' names must be encrypted before being emailed for use at home.
- Documents containing pupils' names will not be saved on any memory stick. If staff wish to work on documents at home they need to be encrypted and then emailed or saved to the hard drive of their allocated laptop.

ICT access

- All staff will be given the School e-Safety Policy and its importance explained.
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- The school will keep an up to date record of all staff and pupils who are granted Internet access.
- Staff may take their laptop and iPad out of school for use at home once they have signed the appropriate paperwork.
- No pupils will be permitted to take any ICT devices out of school.
- Pupils' access to the Internet will be under adult supervision at all times.
- Everyone will be made aware that Internet traffic can be monitored and traced to the individual user.
- E-safety rules will be posted in all rooms where there is computer access and discussed with the pupils at the start of each year.
- Pupils will be informed that network and Internet use will be monitored.
- Parents' attention will be drawn to the School e-Safety Policy in newsletters and on the school website.
- 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 LA ICT can accept liability for the material accessed, or any consequences of Internet access.
- Complaints of Internet misuse will be dealt with by the Head Teacher.

Responding to incidents of misuse

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:

If any apparent or actual misuse appears to involve illegal activity:

- **child sexual abuse images**
- **adult material which potentially breaches the Obscene Publications Act**
- **criminally racist material**
- **other criminal conduct, activity or materials**

Do not shut down the machine but do disconnect the monitor from the mains/close the lid on the laptop and inform the Head teacher immediately. The Head teacher will decide on the severity of the misuse. If there has been illegal misuse the Head teacher will report the incident to the police.

If the misuse is not found to be illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.
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.

Students / Pupils	Actions / Sanctions					
Incidents:	Refer to class teacher / tutor	Refer to Key Stage Leader	Refer to Headteacher	Refer to technical support staff for action	Inform parents / carers	Warning
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			x			
Unauthorised use of non-educational sites during lessons	x					x
Unauthorised use of mobile phone / digital camera / other handheld device	x					x
Unauthorised use of social networking / instant messaging / personal email	x			x	x	x
Unauthorised downloading or uploading of files	x					x
Attempting to access or accessing the school network, using another student's / pupil's account	x					x
Attempting to access or accessing the school network, using the account of a member of staff	x		x			
Corrupting or destroying the data of other users			x			
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			x		x	
Continued infringements of the above, following previous warnings or sanctions			x		x	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			x		x	
Accidentally accessing offensive or pornographic material and failing to report the incident	x		x	x	x	
Deliberately accessing or trying to access offensive or pornographic material			x	x	x	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	x		x	x		x