

E-Safety Policy
Nursling C of E Primary School
Date of Issue: Oct 2017
Review date: Oct 2018



Rationale

Within this school we recognise the importance of ICT and therefore the need to create a safe environment for the whole school community.

The purpose of this policy is to define safe practice for the whole school. The school will ensure that all members of the school community are aware of the e-safety policy and the implications for the individual. E-safety depends on staff, governors, parents and, where appropriate, the pupils themselves taking responsibility for the use of Internet and other communication technologies.

Teaching and Learning

Why is the internet important?

- The Internet is an essential element in 21st century life for education, business and social interaction. Nursling Primary School has a duty to provide pupils with quality internet access as part of their learning experience.
- Providing access to the internet in school will raise educational standards and support the professional work of staff.
- Internet use will enhance learning
- The school internet access is designed for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what internet use is acceptable and what is not and are given clear objectives for Internet use.
- Pupils are educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils are shown how to publish and present information to a wider audience.

Ensuring Internet Access is appropriate and safe.

The following key measures are in place to help ensure that pupils are not exposed to unsuitable material:

- Internet access is purchased from Agile ICT which provides a service designed for pupils including a firewall filtering system intended to prevent access to material inappropriate to children.
- Children using the internet will either be working with an adult, closely supervised or with the permission of an adult, with knowledge of the intentions of the pupil's use of the internet.
- Staff will check that sites are suitable and age appropriate for pupils.
- Impero will be used as a secondary layer of filtering with the ability for teachers to view whatever is on the pupil's device.
- When carrying out research staff will guide pupils to appropriate websites beforehand.
- Pupils will be taught to use email and the internet responsibly in order to reduce the risk to themselves and others.
- Internet safety rules will be displayed clearly in all common areas containing computers with access to the internet.
- The ICT leader will monitor the effectiveness of internet access strategies and will be responsible for raising awareness of safer internet usage.
- School leaders will ensure that the policy is implemented effectively.
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues, advice from the LA, our ISP and the DCFS.

It is not possible to guarantee 100% that particular types of material will never appear on a computer screen. Neither the school nor Hampshire County Council can accept liability for the material accessed, or any consequence thereof.

Most importantly, pupils will be taught to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Access to the Internet

- Pupils have access to computers iPads and laptops in classrooms.
- The internet is filtered by Agile who are our service providers. However no filtering system is 100% so children are encouraged to report any inappropriate material to a relevant adult (Teacher/Teaching Assistant.)
- Pupils are encouraged to 'think smart' about the potential dangers of the internet.
- Pupils are taught about safe use of the internet at an age appropriate level and reinforced across the school.
- Pupils are reminded of the rules in place for safer internet usage.
- The school uses guidance from Hantsweb online safety recommendations as detailed below:

Key Stage 1

Think then Click

These rules help us to stay safe when I go online:

- I only go online with a grown up.
- I am kind online.
- I keep information about me safe.
- I only talk to people online who I know in real life.
- I tell a grown up if something online makes me unhappy.



Key Stage 2

Think then Click

- We ask permission from an adult before using the Internet.
- We only use websites and search engines that an adult has chosen.
- I always talk to an adult if I'm not sure about something or if something happens online that makes me feel worried or frightened.
- I will not use technology to be unkind to people.
- I will only post pictures or videos on the Internet if they are appropriate and if I have permission
- We immediately close any web page we are not sure about.
- We never give out personal information or passwords.
- We don't talk to people online unless we know them in real life.
- We never arrange to meet anyone we don't know.
- I have read and talked about these rules with my parents/carers

Internet Safety Rules

- I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' or teachers permission.
- I will tell my parents or teacher right away if I come across any information that makes me feel uncomfortable.
- I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother, father or guardian along.
- I will never send a person my picture or anything else without first checking with my parents or teacher.
- I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents or teacher right away so that they can take action on my behalf.
- At home I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.
- I will not give out my Internet password to anyone (even my best friends) other than my parents.
- I will be a good online citizen and not do anything that hurts other people or is against the law.

These rules are clearly displayed where computers are made available for the use of pupils. Any pupils who breach any of the above will be dealt with accordingly depending on the severity of the breach ranging from a warning to having internet access denied.

Staff

All staff have access to the school network (which includes internet and e-mail access). Internet access is on 24 hours a day and staff can access the internet and e-mail at any time. Staff may use the internet or e-mail service for professional or private use. Private use is encouraged as it leads to greater professional skills.

All staff internet and e-mail use is subject to the following provisions:

- There is no use of the school network to access inappropriate sites or information such as pornographic, racist or offensive materials
- Users are responsible for all e-mails sent and any contacts made that may result in e-mails being received
- In the case of spam e-mails being received of an offensive manner all such incidents should be reported to the network manager who will take appropriate action.
- No other user should have his or her system or data compromised through deliberate acts by any member of staff.
- No anonymous e-mail or chain e-mail will be forwarded
- No use is made of e-mail or the internet service for mass advertising, political canvassing or gambling.
- Copyright of material is respected
- Use of the internet and e-mail for personal reasons is limited to time when a member of staff is not teaching or supervising pupils
- Downloading of data is permissible providing the user has a legal claim to it.
- Staff are able to work remotely from home on to the school's network, all of the above provisions should be taken into account and abided by. No data from the school network should be copied on to an external non-school device.

Any breach of these provisions will be dealt with according to the severity of the breach. If the breach is a breach of law, the police will be called in straight away and all evidence will be preserved even to the non-use of the school network. If the breach is less severe school disciplinary action would result through established channels