Be the best you can be, every day

ONLINE SAFETY POLICY

Introduction

THIS DOCUMENT IS a statement of the aims, principles and strategies for online safety at North Downs Primary School.

IT WAS DEVELOPED through a process of consultation with teaching and non-teaching staff and Governors.

IT WAS APPROVED BY Governors in Summer Term 2017

THIS POLICY WILL NEXT BE REVIEWED in Summer Term 2018

E-safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for behavior and bullying, safeguarding and child protection, photography and images, and the Privacy notice- Data Protection Act.

Using this policy

- The school has an e-safety committee and has appointed online-safety co-ordinators.
- Members of the online-safety committee have been CEOP (Child Exploitation and On line Protection centre) trained.
- The online-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site, regardless of ownership of the devise.
- The online-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked and appropriate teaching practice is employed to ensure continued e-safety.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by personal passwords.
- The security of school IT systems will be reviewed regularly.

- All staff that manage filtering systems or monitor IT use will have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Internet Use

- The school will provide an age-appropriate online-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.
- Pupils will be strongly advised not to give out personal details or information which may identify them or their location

E-mail

- Pupils and staff may only use approved e-mail accounts on the school IT systems.
- Staff to pupil or families email communication must only take place via a school email address or a school authorised system.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known
- Personal email accounts will not be used for school related content.

Published content e.g. school web site,

- The contact details will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Written permission will be obtained from parents or carers before photographs or names of pupils are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children.

Use of social media

- The school will control access to social networking sites (e.g. Facebook, Twitter, Snapchat and Instagram). This control may not mean filtering or blocking every site; it may mean monitoring and educating students in their use according to the national curriculum.
- The children are taught that they should not access any site, including video and social networking sites, with relevant age restrictions (e.g. Facebook, Twitter, Snapchat and Instagram which all have a recommended age of 13 and above).
- Use of video services such as Skype, will be monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call.
- Staff and pupils should ensure that their online activity, both in and out of school takes into account the feelings of others and is appropriate for their situation as a member of the school community.

Use of personal devices

- Personal equipment may be used by staff to access the school IT systems provided their use complies with the e-safety policy and the relevant AUP.
- Staff must not store images of pupils or pupil personal data on personal devices.

- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Protecting personal data

- The school has a separate 'Privacy notice- Data Protection Act'. It covers the use of biometrics in school, access to pupil and staff personal data on and off site, remote access to school systems.

Policy Decisions

Authorising access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff AUP' before accessing the school IT systems.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- At Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- At Key Stage 2, access to the internet will be with teacher permission and supervision with increasing levels of autonomy.
- People not employed by the school must read and sign a Guest AUP before being given access to the internet.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access.

Handling e-safety Complaints and Incidents

- Complaints of internet misuse will be managed alongside the School Behaviour Policy.
- Complaints of a child protection nature will be managed in accordance with school child protection procedures.

Communication of the Policy

To pupils

- Pupils must agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet
- Pupils will be reminded regularly about the contents of the AUP as part of their e-safety education

To staff

- All staff will be shown where to access the online-safety policy and its importance explained.

- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet
- All staff will receive online-safety training on an annual basis

To parents

- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.
- Parents' and carers' attention will be drawn to the School online-safety Policy in newsletters, the school brochure and on the school web site.
- Parents will be offered online-safety training annually

This policy has links to:

Behaviour policy

Safeguarding & Child Protection policy

Signed…….. Chair of Governors

Date…….