

<u>E-SAFETY POLICY</u>		
<u>May 2017</u>		
Responsibility:	Rachel Moxley and Anna Durbridge	
Review Date:	May 2019	

Based on SCC Model Policy

Rationale

Our e-safety Policy has been written by the school and Children's Centre, building on best practice and government guidance. The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide children with quality Internet access as part of their learning experience.

Aims

Dovers Green School and Children's Centre will use the internet to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the management information and business administration systems. The use of the internet is part of the statutory curriculum and a necessary tool for staff and pupils. Internet access is an entitlement for children who show a responsible and mature approach to its use. The school will seek to ensure that the use of internet derived materials by staff and by children complies with copyright law. Children are taught how to use Hector Protector, an internet security icon if they are worried about anything they see on the screen.

Managing Internet Access

Information System Security

- School and Children's Centre ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly by Dovers Green ICT technician.
- The school and Children's Centre will work closely with the LA to ensure information system security.

E-mail

- Staff may only use approved e-mail accounts on the school and Children's Centre system.
- Children must immediately tell a teacher if they receive an offensive e-mail.
- Children must not reveal personal details of themselves or others in e-mail communication, or via a personal web space, such as an address, or arrange to meet anyone.
- Personal e-mail or messaging between staff and children should not take place.
- E-mails that children send to an external organisation should be written carefully and authorised by an adult before sending, in the same way as a letter written on school headed paper.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Published Content, Children's Images and Work on the Websites

- The contact details on the website should be the school or Children's Centre address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Written permission from parents or carers will be obtained before photographs of children are published on the school or Children's Centre website.
- On the school website only christian names and if necessary the initial letter of the surname will be used for a child's work. There will be no names associated with photographs.
- Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social Networking

- The only social networking site within Dovers Green School is Dovers Green PTA which has the school logo. The Children's Centre staff have access to social networking for promotions and communicating with 'families less likely to engage'.
- Staff should not have children or parents as friends on social networking sites.
- Any use of social networking sites by staff must be considered carefully and used appropriately and professionally. There must be no mention of any aspect of Dovers Green School and Children's Centre.

Managing Filtering

- Dovers Green School and Children's Centre will work in partnership with Surrey County Council and the internet service provider to ensure systems to protect children are reviewed and improved.
- If staff or children come across unsuitable on-line materials, the site must be reported to the ICT technician.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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 phones and associated cameras will not be used during lessons or formal school time except in exceptional circumstances.
- The Children's Centre staff have work mobile phones due to the nature of their roles and their work with families.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet Access

- All staff must read and sign the 'Acceptable Use Policy' before using any ICT resource.
- Dovers Green School and Children's Centre will maintain a current record of all staff and children who are granted access to school ICT systems.
- All parents must read and sign the information relating to ICT in the Pupil Booklet that they receive before starting at the school.
- Access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Any person not directly employed by the school will be asked to sign the 'Acceptable Use Policy' before being allowed to access the internet from the school site.

Assessing Risks

- Dovers Green School and Children's Centre 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 Dovers Green School and Children's Centre nor Surrey County Council can accept liability for the material accessed, or any consequences of internet access.
- Dovers Green School and Children's Centre will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by the headteacher.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with Dovers Green School and Children's Centre child protection procedures.

- Children and parents will be informed of the complaints procedure.
- Children and parents will be informed of consequences for pupils misusing the Internet.

Communications Policy

Introducing the e-safety Policy to Pupils

- Appropriate elements of the e-safety policy will be shared with children.
- 'Think then Click' e-safety rules will be displayed in all networked rooms.
- Children will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for the children.

Staff and the e-safety Policy

- All staff must accept the terms of the 'Acceptable Use Policy' before using any ICT equipment and any internet resource in school.
- All new staff will be taken through the key parts of this policy as part of their induction.
- All new staff will be made aware of this policy.
- All staff including teachers, supply staff, Children's Centre staff, teaching assistants and support staff, will have access to the e-safety policy and have its importance explained.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting Parents' Support

- Parents' and carer's attention will be drawn to the e-safety policy on the websites.
- Parents and carers will from time to time be provided with additional information on e- safety and will be invited to attend curriculum evenings for more information. This could include demonstrations, practical sessions and suggestions on safe internet use at home.
- The school will ask all new parents to sign the information relating to ICT in the Pupil Booklet that they receive before starting at the school.

Planning and Teaching Strategies

- Please refer to the Computing Policy.
- At school, children use the internet under the supervision of teachers and teaching assistants. Additionally in school a filter system blocks access to sites that are inappropriate for little children.
- All children will be reminded of e-safety rules using the 'Think then Click' laminated sheet which is displayed near all computer stations.
- The children will be taught about 'Hector Protector' and how the dolphin icon can be clicked on if children access any inappropriate material.

This curriculum policy should be read in conjunction with *Dovers Greens*

Computing Policy
 Acceptable Use Policy
 Learning and Teaching Policy
 Early Years Foundation Stage Policy
 SEND Policy
 Health and Safety Policy
 Equal Opportunities Policy