ONLINE SAFETY POLICY
(formerly e-safety policy)

Responsibility: Lauren Harvey

Review Date: April 2027

Rationale
Our Online Safety Policy has been written by the school 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 pupils with quality Internet access as part of their learning experience.

Aims
Dovers Green School 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
The school aims to:

- Provide pupils with safe access to age-appropriate online resources.
- Develop children's understanding of online safety through the curriculum.
- Promote safe, respectful and responsible use of technology.
- Protect children from online risks including inappropriate content, contact, conduct and commercial exploitation.
- Ensure staff use technology professionally, safely and legally.
- Safeguard personal data in accordance with UK data protection legislation. [gov.uk], [gov.uk]

Roles and Responsibilities

Governing Body

The Governing Body will:

- Ensure appropriate filtering and monitoring systems are in place.
- Review online safety arrangements regularly.
- Ensure online safety forms part of safeguarding governance.

Headteacher

The Headteacher will:

- Lead implementation of this policy.
- Ensure appropriate staff training is provided.
- Ensure online safety incidents are managed appropriately.

Designated Safeguarding Lead (DSL)

The DSL will:

- Act as the lead professional for online safety safeguarding concerns.
- Maintain records of online safety incidents.
- Liaise with external agencies where required.
- Support staff responding to online safety concerns.

Staff

All staff will:

- Follow the school's Acceptable Use Policy.
- Complete online safety and safeguarding training.
- Report any concerns immediately to the DSL.

Artificial Intelligence (AI)

The school recognises that Artificial Intelligence (AI) tools are becoming increasingly available and may be used by staff and pupils.

Staff Use of AI

Staff may only use AI systems that have been approved by the school for educational or administrative purposes.

Staff must not:

- Enter personal, confidential or safeguarding information into public AI systems.
- Upload pupil data, assessments, reports or photographs into AI tools unless specifically authorised and compliant with data protection requirements.
- Rely solely on AI-generated content without checking accuracy and suitability.

Any AI-generated content used for teaching or communication should be reviewed by a member of staff before use.

Pupil Use of AI

Where AI tools are used with children:

- The activity must be age-appropriate.
- Children must be supervised.
- Staff must discuss safe and responsible use.
- The educational purpose and risks must be considered before use.

The school will assess AI technologies before introducing them into teaching and learning. Recent DfE online safety guidance specifically highlights the need to consider AI within filtering, monitoring and safeguarding arrangements. [saferinternet.org.uk], [gov.uk]

Managing Internet Access

Information System Security

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly by Dovers Green through IT support (Eduthing.)

E-mail

- Staff may only use approved e-mail accounts on the school 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 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 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

- Any official school social media accounts must be authorised by the Headteacher and managed in accordance with school procedures.
- 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.

Managing Filtering and monitoring

- The school maintains filtering and monitoring systems to help protect pupils and staff from harmful online content. The school uses 'Untangle' as its provider.
- Filtering systems will:
    - Block access to illegal content.
    - Restrict access to inappropriate and harmful material.
    - Support safe learning while minimising disruption to educational activities.
- Monitoring systems will:
    - Help identify safeguarding concerns.
    - Support the detection of harmful online behaviours.
    - Generate alerts where appropriate.

Filtering and monitoring systems will be reviewed at least annually and following any significant safeguarding incident, change in technology provision or updated DfE guidance.

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.

Protecting Personal Data
The school will process personal data in accordance with:
- UK GDPR
- Data Protection Act 2018
- School Data Protection Policy

All staff are responsible for protecting personal data and reporting actual or suspected data breaches immediately.

Authorising Internet Access
- All staff must read and sign the 'Acceptable Use Policy' before using any ICT resource.
- Dovers Green School 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 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. Dovers Green School can accept liability for the material accessed, or any consequences of internet access.
- Dovers Green School will audit ICT use to establish if the Online safety policy is adequate and that the implementation of the Online 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.

Responding to Online Safety Concerns
Any online safety concern involving a child must be treated as a safeguarding concern where appropriate.
Concerns may include:
- Online grooming
- Exposure to harmful content
- Cyberbullying
- Sharing of inappropriate images
- Extremist material
- Online scams
- AI-generated harmful content

Staff must report concerns to the Headteacher or DSL immediately.
The school will follow safeguarding procedures and, where necessary, involve external agencies.

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 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 Online Safety Policy to Pupils

- Appropriate elements of the Online 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 Online safety issues and how best to deal with them will be provided for the children.

Staff and the Online 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, teaching assistants and support staff, will have access to the Online 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 Online Safety Policy on the websites.
- Parents and carers will from time to time be provided with additional information on online 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.

Monitoring and Review

This policy will be reviewed annually by the Headteacher, Designated Safeguarding Lead and Governing Body or sooner following significant changes in legislation, statutory guidance, technology or safeguarding practice.

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