



# **Shawlands Primary School**

## **Policy**

**Online Safety Policy**  
**REVIEWED EVERY 3 YEARS**

**Reviewed by B Hitchen Spring 2020**

**Approved by the Governing Body on:**

**Signed.....**



# SHAWLANDS PRIMARY SCHOOL

## E-Safety POLICY



### 1 INTRODUCTION

At Shawlands Primary School we understand the responsibility we have to educate our pupils on Online Safety issues; teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Shawlands Primary School has a whole school approach to the safe use of ICT and creating this safe learning environment includes three main elements:

- an effective range of technological tools
- policies and procedures, with clear roles and responsibilities
- a comprehensive online safety programme for pupils, staff and parents.

This policy has been contributed to by the whole school and ratified by the governors.

For expectations regarding the taking, distribution and publication of photography and videos at Shawlands see the photography and CCTV policy.

This policy is to be read in conjunction with all other policies particularly: Behaviour Policy, Safeguarding Policy and Child Protection Policy, Code of Conduct policy, Photography and Video Policy, and Equal Opportunities Policy.

### 2. DEFINITION OF E-Safety

The ability to use ICT is an important curriculum requirement and a vital skill in modern society. We interpret the term ICT to include the use of any equipment which allows users to communicate, manage, code or manipulate information electronically.

### 3. ROLES & RESPONSIBILITIES

E-Safety is recognised as an essential aspect of strategic leadership in Shawlands Primary School. All staff on the Child Protection team have received CEOP (Child Exploitation and Online Protection) training.

Mr D Thompson (Headteacher) has overall responsibility. Mrs Hill and Mr Hitchen are the named staff for children to report any concerns.

It is the role of these staff members to keep abreast of current issues and guidance through organisations such as BMBC, Becta, CEOP (Child Exploitation and Online Protection), and Child Net. The Head teacher ensures Senior Management and Governors are updated as necessary. All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.

All staff should be familiar with the school's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs on the school website
- procedures in the event of misuse of technology by any member of the school community
- their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety regularly and new staff receive information on the school's acceptable use policy as part of their induction.

Managing the school e-safety messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.

- The e-safety policy will be shared with new staff and students, including the acceptable use policy as part of their induction.

- E-safety posters will be prominently displayed.

#### **4 THE CURRICULUM**

Computing and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new ways to promote e-safety.

- We provide opportunities within a range of curriculum areas to teach about e-safety.

- Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise and as part of the curriculum.

- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling, and activities as part of the ICT curriculum.

- We regularly distribute questionnaires to children to monitor their understanding of e-safety.

- Pupils are aware of the impact of online bullying through PSHE and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

#### **5 MANAGING INTERNET ACCESS**

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education as well as a potential risk to young people.

Students will have supervised access to Internet resources through the school's fixed and mobile internet technology.

Staff will preview any recommended sites before use.

Raw image searches are discouraged when working with pupils.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise any further research.

Our internet access is controlled through an appropriate and recommended web filtering service. Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety co-ordinator and an email sent to the network manager so that they can block the site.

It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

Any changes to filtering must be authorised by a member of the senior leadership team.

## **6 SECURITY AND DATA PROTECTION**

The school and all staff members comply with the Data Protection Act 1998. Personal data will be recorded, processed, transferred and made available according to the act. Password security is essential for staff, particularly as they are able to access and use pupil data. Staff have secure passwords which are not shared with anyone. All families have been given and signed an eSafety agreement and had an invitation to a full training session.

## **7 E-SAFETY COMPLAINTS AND INCIDENTS**

As a school we take all precautions to ensure e-safety at all times. However, due to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device. The school cannot accept liability for material accessed or any consequences of this. Complaints should be made to the Headteacher. Incidents should be logged and the flowchart for managing an e-safety incident is to be followed. It is important that the school work in partnership with pupils and parents to educate them about Cyber bullying and children, staff and families need to know what to do if they or anyone they know are a victim of Cyber bullying. All bullying incidents should be recorded and investigated via the incident log form.

## **8 REVIEW OF POLICY**

There are on-going opportunities for staff, children and families to discuss e-safety concerns with our Learning Mentors. This policy needs to be reviewed every 3 years and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or any guidance or orders are updated.

**Shawlands Primary School**  
**Spring 2020**