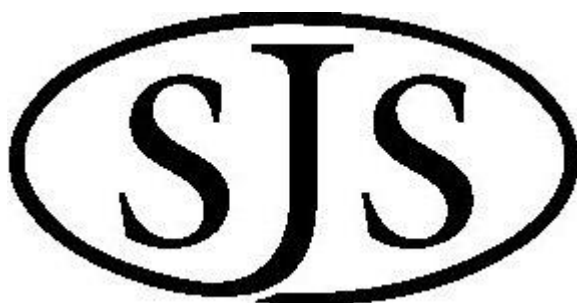


# Shaftesbury Junior School

## E-Safety Policy



*'We care, we share, for the future we prepare'*

**Approved by:** Headteacher

**Date:** 23<sup>rd</sup> June 2025

**Last reviewed on:** June 2025

**Next review due by:** June 2026

This policy reflects requirements for inclusion and equality as set out in the [Special Educational Needs and Disability Code of Practice 2014](#) and [Equality Act 2010](#), and refers to curriculum-related expectations of governing boards set out in the Department for Education's [Governance Handbook](#).

We support the 'City of Sanctuary' vision that the UK will be a welcoming place of safety for all and proud to offer sanctuary to people fleeing violence and persecution. We endorse the City of Sanctuary Charter, and agree to act in accordance with City of Sanctuary values and apply the network principles within our work.

We recognize the contribution of people seeking sanctuary. Sanctuary seekers are welcomed, included and supported within our context.

## **Statement of intent**

The purpose of this policy is to ensure that all staff, parents, governors and children understand and agree the school's approach to e-safety. The policy relates to other policies including ICT curriculum, Internet Access, Bullying, Safeguarding and Health and Safety.

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

### **Internet use will enhance learning**

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils;
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use;
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge retrieval and evaluation.

### **Pupils will be taught how to evaluate Internet content**

- The school will ensure that the use of the Internet derived materials by staff and pupils complies with copyright law;
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

## **Managing Internet Access**

### **Information system security**

- School ICT systems capacity and security will be reviewed regularly;
- Virus protection will be updated weekly;
- Software updates will be checked weekly.

### **Email content and the school website**

- Pupils may not use email in the school;
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.

### **Publishing pupils' images and work**

- Photographs that include pupils will be selected carefully;
- Pupils' full names will not be used anywhere on the website;
- Written permission from parents/ carers will be obtained before photographs of pupils are published on the website.

## Social networking and personal publishing

- The school will deny access to social networking sites and students will be advised about appropriate use of these;
- The school will run its own social networking sites conforming to the Social Media Policy.

## Managing filtering and monitoring

- The school will work with the LA, DfE and the Internet service provider to ensure systems to protect pupils are reviewed and improved;
- If staff or pupils discover an unsuitable site, it must be reported to the ICT Co-ordinator;
- IT provider runs regular checks on the filtering and monitoring software and reports to governors on a monthly basis;
- There is a nominated governor with responsibility for filtering and monitoring;
- A live test of the filtering and monitoring software is carried out at each full governing body meeting.

## Assessing risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access. The school will teach pupils how to proactively manage any inappropriate material that is found.

## Handling e-safety complaints

- Complaints of Internet misuse will be taken seriously and investigated;
- Any complaint about staff misuse must be referred to the Headteacher;
- Complaints of a child protection nature must be dealt with in accordance with the school's Safeguarding Procedures.

## Staff and the E-safety policy

- All staff will have access to the E-safety Policy and understand its importance;
- Staff should be aware that Internet traffic could be monitored;
- Discretion and professional conduct is essential.

## Working with parents

- Parents' attention will be drawn to the E-safety Policy;
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location;
- Pupils will be made aware of how they can report abuse and who they should report it to;
- Pupils will be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future;
- Pupils will be made aware of the dangers of social media and mobile apps, particularly around grooming and sexting;
- Pupils will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications;
- Pupils will be taught to only invite known friends and deny access to others.