

# Shakespeare

Primary School

**Shakespeare Primary School**

**E-safety Policy**

**2023-2025**

Our E-Safety Policy has been written by the school, building on the Leeds E-Safety Policy and government guidance. It has been agreed by the staff and approved by the governors.

## **Teaching and Learning**

### **Why internet use is important**

- 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 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 location, retrieval and evaluation.

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

- The school will try to ensure that the use of internet-derived materials by staff and pupils complies with copyright law.
- Pupils should 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 regularly. Staff should ensure virus protection is updated on laptops.

### **E-Mail**

- Pupils may only use approved e-mail accounts on the school system.
- Pupils use DB Primary based emails and can 'blow the whistle' if they receive offensive e-mail. This will notify a member of the leadership team and be dealt with appropriately following school policy.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.

- The forwarding of chain letters is not permitted.

### **Published content and the school web-site**

- The contact details on the web-site 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.

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

- Pupils' full names will not be used anywhere on the web-site or blog.
- Photos and work will only be published where consent has been sought.

### **Social networking and personal publishing**

- ICT4Leeds will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school should be closely monitored and age recommendations strongly considered

The key messages delivered to pupils are:

- Don't post personal information or personal pictures of you online where everyone can see it.
- Keep your username and passwords secret.
- Don't send emails or messages to people you don't know.
- Don't open emails or messages to people you don't know.
- Be kind and polite, treat people how you would like to be treated yourself.
- If you are not sure then ask an adult you trust.

### **Managing filtering**

- The school will work with the ICT4Leeds to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to Computing Team Leader and or senior member of staff.

### **Protecting personal data**

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


### **Policy Decisions**

#### **Authorising internet access**

- The school will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date.
- At Key Stage 1, access to the internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Children will only access the internet when an adult is present.

### Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate 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. Neither the school nor Children Leeds can accept liability for the material accessed, or any consequences of internet access.
- The school will audit ICT provision to establish if the E-Safety Policy is adequate and that its implementation is effective.
- All school staff will be supported in using the Four Cs to classify risk

 <b>Content</b> Child as recipient	<b>Contact</b> Child as participant	<b>Conduct</b> Child as actor	<b>Contract</b> Child as consumer	
<b>Aggressive</b>	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
<b>Sexual</b>	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
<b>Values</b>	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
<b>Cross-cutting</b>	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

## **Handling e-safety complaints**

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

## **Communications Policy**

### **Introducing the E-Safety Policy to pupils**

- E-safety rules will be posted in all networked rooms
- Lesson 1 of each half term will be based on the government Thinkuknow resource
- Pupils will be informed that network and internet use will be monitored and shown how to seek help if they feel they need it.
- Dside will support in delivering online safety sessions to all KS2 pupils.

### **Staff and the E-Safety Policy**

- All staff will be given access to the School e-Safety Policy and 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.
- Training will be available to those who request or require it.

### **Enlisting parents' support**

- Parents' attention will be drawn to the school's E-Safety Policy in newsletters and on the school web-site and through the effort of Esafety week.