



## **St Mary's RC Primary School**

### **Online Safety Policy**

#### **Rationale**

E-Safety encompasses internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

This policy has been written by St Mary's RC Primary School with Government and authority guidance. This policy will also operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data protection, Safeguarding and Child Protection.

The Head Teacher will also act as the Internet Safety lead.

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

The purpose of internet use in schools is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.

#### **Good Habits**

- Responsible ICT use by all staff and pupils; encouraged by education and made explicit through published policies
- Sound implementation of E-safety policy in both administration and curriculum, including secure school network design and use
- Safe and secure broadband including the effective management of content filtering

#### **Internet access**

- If staff or pupils discover an unsuitable site, it must be reported to the ICT subject leader
- The Internet is for educational use only during school hours
- Children will only access the Internet at school under adult supervision

- Internet access will be planned to enrich and extend learning opportunities
- Access levels will be reviewed regularly to reflect the curriculum requirements and ages of pupils
- Staff should guide pupils in on-line activities
- Pupils will be taught effective Internet search techniques, including the skills of knowledge location, evaluation and retrieval
- Teachers should ensure that the use of Internet derived content complies with copyright law
- All staff must read and sign the Acceptable Internet Use agreement before using any school ICT resource
- Parents will be asked to sign and return a consent form for pupil Internet access

### **Email**

- No member of staff should engage in direct communication (in or out of school) with a pupil
- Pupils may only use approved email accounts within school
- Pupils must immediately tell an adult if they receive an abusive email
- Pupils must not reveal personal details or arrange meetings via electronic communication
- Education about Internet safety will be covered as part of the ICT curriculum
- The forwarding of chain letters or mail is not permitted

### **Social networking**

- Access to social networking sites and newsgroups is not permitted unless a specific use is approved
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils will be advised not to place personal photographs on any social network space
- Pupils will be advised and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils will be encouraged to invite known friends only and deny access to others
- Pupils will be advised what to do about sexting (the sending or receiving of sexually explicit images or videos). Guidance on how to deal with sexting can be found at:  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/551575/6.2439\\_KG\\_NCA\\_Sexting\\_in\\_Schools\\_WEB\\_1\\_.PDF](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB_1_.PDF)

### **School website and Facebook Page**

- Pupils' full names will not be used on the school website or Facebook page
- Written permission will be obtained from parents/carers before photographs of pupils are published on the school website or Facebook page

### **Visual and audio technology**

Pupils will always seek the permission of teachers before making audio/visual recordings within school and will work under the supervision of an adult.

### **Filtering**

The school will work in partnership with the Local Authority and Internet provider to ensure filtering systems are as effective as possible. This is currently a centrally hosted web filtering provision enabling safe internet access for schools. This provides school with the flexibility to locally manage and control access to websites. School runs a monthly filtering test to check that the filter remains secure.

### **Mobile phones**

Mobile phones will not be used during the school day by pupils. Pupils who bring mobile phones to school should hand them into the main school office for safe keeping at the start of the day and then collect them when school ends. Staff in school will only use digital cameras or ipads which have been provided by school and staff mobile phones are not permitted for use anywhere in school around the children. This also applies to all visitors to school. Staff mobile phones may only be used in the staffroom and office areas. The only exception to this is when staff carry mobile phones on school trips in case of emergencies.

### **Emerging technologies**

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

### **The prevent duty and online safety**

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the Internet in school. School has an important part to play in equipping our children to stay safe online. Internet safety is integral to our computing curriculum. Staff are aware of the risks posed by online activity of extremists and we have a duty to take action if they believe the welfare of any pupil is compromised.

### **How will the risks be assessed?**

To guard against accidental and inappropriate materials, St Mary's RC Primary School accesses the Internet via the Lancashire Grid for Learning, which provides an appropriately filtered service (including Google). If however, unsuitable material is found on school devices, the URL and content must be

reported to the ICT subject leader who will inform the Internet Service Provider, in order for the site to be blocked.

### **How will ICT system security be maintained?**

- Internet use by pupils in school will always be supervised by a staff member
- Filtering software/systems will be used to reduce the risk of exposure to unsuitable material
- Pupils and staff will be provided with training and regular updates in the area of Internet safety
- Virus protection software will be used and updated regularly
- The school network is regularly maintained and monitored by competent technical support

### **Handling Internet Safety Complaints**

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaints of staff Internet misuse MUST be referred to the Headteacher
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures

### **Policy decisions**

- All staff should be aware of and adhere to the principles laid out in this policy
- The school will keep a record of all staff and pupils in school who are granted Internet access. This record must be kept up to date.
- Visitors to school will only be allowed supervised or limited access to the Internet.
- Parents will be given a copy of the Acceptable Internet Use Form to consent to their child accessing the Internet safely within school. Pupils will also be asked to sign the form.

### **Online Safety Training**

All teachers have completed an online safety training course.

### **Staff**

- All staff will be given the Online Safety Policy and its importance explained
- All staff will be trained in safeguarding procedures, including elements of Online Safety and The Prevent Duty
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential

- All staff will read and sign to say they have understood the Staff Information Systems Code of Conduct (this forms part of the induction process for new staff).

Signature from Governors: *[Handwritten Signature]* Date: Sept 2022

Signature of Head teacher: *Claire Halstead* Date: Oct 2022

Date of next review: September 2023

Policy date – October 2022



All are welcome here to walk with Jesus as we love, learn and flourish.