



## Online Safety Policy

Policy owner/author	Rachael Harfield
Approved by	<u>Headteacher</u>
Statutory policy	<u>No</u>
Review cycle	
Date last reviewed	<u>16 January 2024</u>
Date of next review	<u>16 January 2025</u>
Related policies	Safeguarding policy / PSHE scheme

### Version History Log

Date	Version	Comments/Summary of changes
<u>16/03/2023</u>	1	

### Our Vision Statement 'Learning for Life'

'Learning for life' with Jesus' promise of 'life in all its fullness' is at the heart of St Mary's.

At our school, children are seen as unique and will feel loved, safe and empowered to flourish so they reach their full potential both academically and personally.

### Writing and reviewing the Online Safety Policy

The Online Safety Policy relates to other policies including those for Computing, Anti-bullying, Data Handling, Safeguarding and Child Protection.

- Our Online Safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The Online Safety Policy and its implementation will be reviewed annually.
- The Online Safety Policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site.

### Teaching and learning

#### Why Internet and digital communications are important

- 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.
- 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 is provided by RM Unify and includes filtering appropriate to the age of pupils.



# St. Mary's CofE Primary

## 'Learning for Life'

---

- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use. This is done through both Computing and PSHE lessons.
- 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 seek to ensure that the use of internet derived materials by staff and by pupils complies with copyright law.
- Pupils will be taught how to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught how to report unpleasant internet content.

### **Managing Internet Access**

#### **Information system security**

- School ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Local Authority.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform Online Safety Policy.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.



# St. Mary's CofE Primary

## 'Learning for Life'

---

- Access to school networks will be controlled by passwords.

### **Internet Use**

- The school will provide an age appropriate online safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety.
- Pupils will be advised not to give out personal details or information which may identify them or their location.
- All communication between staff and families will take place using school equipment and / or school accounts.

### **Published content and the school website**

- 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.

### **Publishing pupil's images and work**

- Pupils' full names will not be published by the school on the School Website or learning platform, particularly in association with photographs.
- For more information, please see the "Use of Photography Policy".

### **Social Media**

- The school has a separate Social Media Policy.
- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Pupils will be taught about the dangers of social networking and will be given advice on how to stay safe.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils. Parent workshops around internet safety are provided for Safer Internet Day.
- Pupils will be advised to use nicknames and avatars when using social networking sites.
- All staff, including teaching assistants and office staff, will be strongly advised not to accept or send any communications with pupils via social networking sites outside of school.
- Staff and pupils should ensure that their online activity, both in school and out, takes into account the feelings of others and is appropriate for their situation as a member of the school community.

### **Personal Devices**

- Personal equipment may be used by staff to access the school IT systems provided their use complies with the Online Safety Policy and the relevant AUP.
- Staff must not store images of pupils or pupil personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

### **Managing filtering**

- The school will work in partnership with Surrey County Council to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable online materials, the site must be reported to a member of the Senior Leadership Team and IT support, EduThing, to remove the material from the school's network.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.



# St. Mary's CofE Primary

## 'Learning for Life'

---

### **Managing video-conferencing**

- The supervising teacher will make and answer any video-conference calls.
- Video-conferencing will be appropriately supervised for the pupils' age.

### **Phones, Cameras and Smart Watches**

- Only school cameras should be used by teaching staff and pupils.
- Photographs should be deleted off the camera once uploaded onto a computer.
- Pupils are not allowed to use their own cameras (including camera phones) in school.
- Pupils are not allowed to use mobile phones and smart watches in school.
- If a pupil requires a mobile for their journey to or from school, then this must be handed in with the appropriate completed form to the class teacher at the start of the school day and collected again at home time.
- If a pupil has a smart watch, this must be handed into their class teacher at the start of the school day and collected again at home time.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff will use a school phone where possible to contact parents or carers as required.

### **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.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

### **Protecting personal data**

- Personal data will be recorded, processed, transferred and made available according to the GDPR Data Protection Act 2018.
- The school has a separate Data Handling Policy.

### **Policy Decisions**

#### **Authorising Internet Access**

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff Acceptable Use Policy' before using any school computing resource. This is refreshed each year at our initial INSET day.
- Visitors to the school, who will have access to computing resources, are to sign an Acceptable Use Policy when completing relevant paperwork to visit the school.
- All pupils in KS1 and KS2 must read the Acceptable Use Agreement and Online Code of Conduct before using any school computing resource. This will be done electronically at the start of each academic year.
- The school will maintain a current record of all staff and pupils that have or have not signed the policy.
- Cover teachers will have signed AU agreements as part of the Cover Agency Package.
- Parents will be asked to sign and return a consent form to allow use of technology by their child when they join the school.
- At Key Stage 1 and foundation, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.
- At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.



# St. Mary's CofE Primary

## 'Learning for Life'

---

### Assessing risks

- The 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. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access.
- The school will review computing use to establish if the Online Safety Policy is adequate and that the implementation of the Online Safety Policy is appropriate and effective.
- Staff have the right to ban pupils from using any pieces of ICT within school if they feel it has been used inappropriately.
- Parents must be informed if any child is banned from using a piece of ICT within school on a long term basis.

### Handling online safety complaints

- Complaints of internet misuse will be dealt with according to the school Behaviour Policy.
- 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.
- Pupils and parents will be informed of consequences for pupils misusing any ICT equipment.

### Community use of the Internet

- Members of the community and other organisations using the school internet connection will have to sign a Visitor AUP so it is expected that their use will be in accordance with the school Online Safety Policy.

### Communications Policy

#### Introducing the online safety policy to pupils

- Pupils need to agree to comply with the pupil AUP in order to gain access to the school IT systems and to the internet.
- Online safety rules will be posted in all networked rooms.
- Pupils 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 pupils.
- Pupils will be reminded about the contents of the AUP as part of their online safety education.

#### Staff and the Online Safety Policy

- All staff will be shown where to access the school Online Safety Policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet, which outlines acceptable use around technology, including but not limited to mobile phones and smart watches.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.
- Staff will receive online safety training on an annual basis.

### Enlisting parents' support

- Parents' and carers' attention will be drawn to the school Online Safety Policy and Acceptable Use guidance in newsletters and on the school website.
- Parents and carers will be given information on online safety each year during Internet Safety Week. Time to time, additional information may also be sent out to parents or put onto the website.



# St. Mary's CofE Primary

## 'Learning for Life'

---

- The school will ask all new parents to sign the parent / pupil agreement when they register their child with the school.

