St Mary's CE (Aided) Primary School
A Christ-centred school with a child-centred curriculum

E-Safety Policy

Updated: September 2025

Up for review: September 2028

In our school our Christian vision shapes all we do.

We treasure each child and enable them to flourish, using their God-given potential, establishing a secure foundation for them to thrive in a rapidly changing world.
We are a 'Christ-centred school, with a child-centred curriculum' where wisdom and love guide and influence learning and teaching for our whole community.

INTRODUCTION

At St Mary's CE Primary School, we take the safety of our pupils very seriously.
E-safety involves pupils, staff, governors and parents making the best use of technology, information, training and this policy to create and maintain a safe online and computing environment for St Mary's Primary School.

As in any other area of life, children and young people are vulnerable and may expose themselves to danger – knowingly or unknowingly – when using the internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or even illegal.
To ignore e-safety issues could ultimately lead to significant gaps on child protection policies, leaving children and young people vulnerable. *(Safeguarding Children in a Digital World, BECTA, 2006)*

The purpose of this policy is to:

• Through consultation with pupils establish the ground rules we have in St Mary's CE Primary School for using the Internet and electronic communications such as mobile phones, 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 experience.

• Describe how these fit into the wider context of our discipline and RHE policies.

• Demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.

• Understand that accessing inappropriate sites accidentally is not something to feel guilty about and that any such incident should be reported to staff immediately.

Safeguarding and online learning

Since March 2020, schools and other educational settings have moved at an exponential rate to develop ways of using technology to facilitate learning and, since October 2020, all settings are legislated to have remote learning provision. The national expectations are outlined in the Remote Education Temporary Continuity Direction guidance.
This is further supported by guidance issued on 7th January 2021 from the Department for Education issued 'Restricting attendance during the national lockdown: schools. Guidance for all schools in England'.1

Keeping Children Safe in Education (KCSIE) 2025

Schools will be aware that the new version of Keeping Children Safe in Education (KCSiE) applies from 1 September 2022. Paragraphs 133 to 138 in the KCSiE document make specific reference to online safety. Other key additions to KCSiE this year include the need for staff to be alert to children's mental health problems as a possible indicator that a child has suffered or is at risk of suffering abuse, neglect or exploitation, and the need for schools to follow up on safeguarding concerns in relation to supply staff.

1. E-SAFETY AT ST. MARY'S CE (AIDED) PRIMARY SCHOOL:

This policy forms part of the School Improvement Plan (SIP) and links to other policies such as Computing, Child Protection, Behaviour and Anti-bullying. It has been created with advice taken from a number of local authorities (West Sussex, Brighton and Hove, Kent and Sheffield) and also government guidance.

E-safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, collaboration tools and personal publishing. E-safety concerns safeguarding children and young people in the digital worlds. It emphasises learning to understand and use new technologies in a positive way and informs about the risks and the benefits. E-safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

E-safety depends on effective practice at a number of levels:

• Responsible ICT use by all staff and students; 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 filtering.

• A member of staff being responsible for the implementation and monitoring of this E-safety policy.

As E-safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The role of E-safety Co-ordinator is part of the Computing Co-Ordinator role, working closely with other members of staff responsible for Child Protection. The named E-safety Co-ordinator in our school is Rachel Sleat. This policy has been agreed by the Senior Leadership Team and approved by the governors.

This policy will be reviewed annually as part of the Safeguarding Review.

2. TEACHING & LEARNING AT ST. MARY'S CE (AIDED) PRIMARY SCHOOL

2.1 The importance of internet use

The purpose of the internet in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. The internet is an essential tool of the 21st century in all walks of life, including business and leisure, therefore schools have a duty to provide pupils with quality internet access as part of their learning experiences.

- The school internet access is designed expressly for pupil use and includes appropriate content filters.
- Pupils are given clear objectives for internet use and taught what is acceptable and what is not.
- Staff will give pupils online activities which enhance learning that are planned for their age and maturity.
- Pupils are educated in the effective use of the internet for research, including the skills of evaluation.
- When children are directed to websites for use at home, they will have been checked for appropriate content by the teacher setting the learning.
- The school will ensure that the use of internet-derived materials by staff and pupils complies with copyright law.
- Pupils are taught the importance of cross-checking information before accepting its accuracy.
- As part of the computing curriculum, all year groups have digital literacy units that focus on different elements of staying safe online. These topics include how to use a search engine, our digital footprint and cyber bullying.
- E-safety is taught in school using Purple Mash and every year we participate in the Safer Internet Day – reiterating the importance of staying safe online.

3. MANAGING INTERNET ACCESS AT ST. MARY'S CE (AIDED) PRIMARY SCHOOL

3.1 Information system security

- Security strategies are reviewed regularly in conjunction with West Sussex County Council; virus protection is updated on a regular basis by the school IT technician.
- Any portable devices should have a virus check before being used in school.
- The school server is backed up each night and if any administrator account passwords become known they will be changed straight away.

- All personal data sent via the internet will be secured or encrypted. Computers, including mobile devices, may not be connected to the school network, physically or wirelessly, without specific permission.
- Personal data, relating to staff or pupils, should not be held on the school server without specific permission and any files held on the server will be regularly checked. No software is to be added or removed from the school network; any software to be added or removed may only be done so by the IT technician.

3.2 Email

- Pupils must only use approved email accounts on the school system. Access to personal email accounts is blocked.
- Pupils must immediately tell an adult if they receive offensive email.
- In any email communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming email should be treated with care and attachments not opened unless the author is known.
- The forwarding of chain letters is not allowed. All chain letters, spam, advertising and emails from unknown sources will be deleted without opening or forwarding.

3.3 School website

- The contact details on the school website are the school address, email and telephone number. Staff and pupils' personal details are not published.
- The Headteacher will take overall editorial responsibility and ensure that the content is accurate and appropriate.
- Photographs that include pupils are selected carefully so they do not enable individual pupils to be clearly identified, unless parental permission has been given.
- Pupils' full names are not used anywhere on the website or blog.
- Written permission from parents or carers must be obtained before photographs of pupils are published on the school website.
- Pupils' work will only be published with the permission of the pupil and parents.

3.4 Publishing of pupil images

- Photographs that include pupils will be selected carefully with the permission of parents / carers/guardians.
- Pupils' full names will not be used anywhere on the school website or other online space, particularly in association with photographs.

- Pupils' work will only be published on the website with permission of the pupil and parents / guardians.
- Parents are clearly informed of the school policy on image taking and publishing, both on the school and independent electronic devices.
- Written permission will be kept for pupils whose parents have allowed images to be published on the school website.

3.5 Social networking

Social networking internet sites provide facilities to chat and exchange information online. The online world is very different from the real one, with the temptation to say and do things that would normally be said and done in face-to-face situations.

- The use of social networking sites in school is not allowed and will be blocked or filtered. Newsgroups are also blocked.
- Pupils are taught not to give out personal details of any kind that may identify themselves, other pupils, their school or location. This also includes photographs and videos.
- Pupils and parents will be advised that the use of social network sites outside of school is inappropriate for primary school-aged children.
- Pupils are encouraged to only interact with known friends, family and staff over the internet and deny access to others.
- Parents, pupils and staff are advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber-bullying and defamatory comments.

3.6 Mobile phones

Smartphones have access to the internet and picture / video messaging. Whilst these are advanced features, they present opportunities for unrestricted access to the internet and sharing images. There are risks of mobile bullying or inappropriate contact.

- Pupils are not to bring mobile phones to school unless given permission by the head teacher where parents have asked for permission for the phone to be present for safety / precautionary use. Pupils' phones should be handed in at the School Office for safekeeping until home time.
- The sending of abusive or inappropriate text messages is forbidden.
- Staff should not use their own personal mobile phones to contact parents. The school phone should be used.
- Staff and visitors are not permitted to use their phones in classrooms, corridors, the school hall, playgrounds, field or Forest School without the express permission of the Headteacher. Staff should turn off their phones, or put them onto silent mode, and store them in a safe place away from children.

- Staff may use their mobile phone in the staffroom or Office to make calls at break times away from pupils. Consideration should be given to other people in these areas when using phones.
- Parents and other volunteer helpers may not use mobile phones or other mobile devices on school trips to take photographs of their own children or other children.

3.7 Cameras and video

Although most cameras are not directly linked to the internet, the images can easily be transferred.

- Pupils will not use cameras unless authorised by staff.
- Publishing of photographs and videos will follow the guidelines set out in sections 3.3 and 3.4 of this policy.
- Parents may use cameras to take images of their own children in school plays / assemblies when the Headteacher gives permission. Images of children taken in school must not be shared on social networking sites.
- Photographs taken by parents must not be published in any manner; they are for private retention only.

4. MANAGING EMERGING TECHNOLOGIES

Technology is a fast-changing industry and the school will endeavour to keep up with new technologies as much as possible within the financial constraints placed upon them. As new technology comes to the forefront, the school will consider it with regards to the educational benefit that it could bring. A risk assessment will be carried out before use in school is allowed.

- The Senior Leadership Team is aware that new technologies such as mobile phones with wireless technology can bypass school filtering systems and present a route to undesirable material and communications. Mobile phones will not be used in lessons or formal school time.

5. PROTECTING PERSONAL DATA

Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.

6. ASSESSING RISKS

The school will take all reasonable precautions to ensure that the users access only appropriate material. However, due to the global and connected nature of the internet, it is not always possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor West Sussex County Council can accept liability for the material accessed, or any consequences resulting from internet use.

- The school will audit computing use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

7. POLICY DECISIONS

Authorising Internet access

- All staff are expected to adhere to 'Acceptable ICT Use Agreement' before using any school ICT resource.
- All pupils in the school are expected to adhere to an Acceptable Use Policy when they join the school, and on commencement of a new Key Stage (Key Stage 2).
- At Key Stage 1, access to the internet will be closely supervised by an adult, with access to specific, approved on-line materials.
- At Key Stage 2, access to the internet will be by supervised access to specific, approved on-line materials.

8. COMMUNICATIONS

Introducing the E-safety policy to pupils

- E-safety rules are posted in all networked rooms and discussed with the pupils at the start of each year linked to the Purple Mash SMART rules (see Appendix 3 for Internet Safety Rules).
- Pupils are informed that network and Internet use will be monitored.
- As part of the National Curriculum and skills development, Key Stage 2 pupils and their parents are informed of the child exploitation and online protection centre:

  www.thinkuknow.co.uk

9.HANDLING E-SAFETY COMPLAINTS

- Complaints of internet misuse will be dealt with by the Headteacher or a senior member of staff in their absence.
- Any complaint about staff misuse must be referred to the Headteacher or governing body.
- Complaints of a child protection nature will be dealt with in accordance with school protection procedures.

- Pupils and parents will be informed of the Complaints Procedure.
- Discussions may take place with Sussex Police to establish procedures for handling potentially illegal issues.

10. STAFF AND THE E-SAFETY POLICY

All staff have access to copies of the school's E-safety Policy and know its importance.

Staff are aware that Internet traffic can be monitored and traced to the individual user.

11.ENLISTING PARENTS' SUPPORT

Parents' attention is drawn to the school's E-safety Policy in newsletters, the school brochure and on the school website.

We hold regular E-safety meetings for parents and carers where support and advice is given using West Sussex County Council materials.

12.CYBER BULLYING

WHAT IS CYBER BULLYING?

- Cyber bullying includes sending or posting harmful or upsetting text, images or other messages, using the internet, mobile phones or other communication technology.
- It can take many forms, but can go even further than face-to-face bullying by invading home and personal space and can target one or more people.
- It can take place across age groups and target pupils, staff and others.
- It can include threats and intimidation, harassment, defamation, exclusion or peer rejection, impersonation and unauthorised publication of private information or images.
- It can include messages intended as jokes, but which have a harmful or upsetting effect.

Cyber bullying may be carried out in many ways, including:

- Threatening, intimidating or upsetting text messages;
- Threatening or embarrassing pictures and video clips via mobile phone cameras;
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible;
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name;
- Menacing or upsetting responses to someone in a chat-room;
- Unpleasant messages sent during instant messaging;
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites

In some cases, this type of bullying can be a criminal offence.

Responding to cyber bullying

Cyber bullying will generally be dealt with through the school's Anti-Bullying Policy. A cyber bullying incident might include features different to other forms of bullying, prompting a particular response. Key differences might be:

- Impact: possibly extensive scale and scope
- Location: the anytime and anywhere nature of cyber bullying
- Anonymity: the person being bullied might not know who the perpetrator is
- Motivation: the perpetrator might not realise that his/her actions are bullying
- Evidence: the subject of the bullying will have evidence of what happened

Investigation

Again, the nature of any investigation will depend on the circumstances. It may include, for example:

- Review of evidence and advice to preserve it, for example by saving or printing (e.g. phone messages, texts, emails, website pages)
- Efforts to identify the perpetrator, which may include looking at the media, systems and sites used. Witnesses may have useful information.
- Contact with the Internet Watch Foundation, the police or the Safeguarding Children
- Police if images might be illegal or raise child protection issues.
- Requesting a pupil to reveal a message or other phone content or confiscating a phone. Staff do not have the authority to search the contents of a phone.

This policy will be reviewed annually by the subject leader for ICT in the light of new guidance and presented to staff and governors.

STAFF CODE OF CONDUCT

To ensure that you are fully aware of your professional responsibilities when using ICT in school, you are asked to read and sign this code of conduct. You should consult the school's E-safety Policy for further information and clarification.

- The ICT systems are school property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- I will ensure that my ICT use will always be compatible with my professional role.
- I understand that ICT may not be used for private purposes, without specific permission from the head teacher.

- I understand that the school may monitor my ICT and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school's E-safety Coordinator or the Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote E-safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Safeguarding when using online approaches:

- We use Google Classroom as our online platform.
- Online learning is an extension of school, therefore the same common principles apply between teachers, parents and pupils.

CYBER SAFETY CODE

Three Steps to Safety

1. Respect other people - online and off. Don't spread rumours about people or share their secrets, including phone numbers or passwords.

2. If someone insults you online or by phone, stay calm. Ignore them, but tell someone you trust.

3. "Do as you would be done by!" Think how you would feel if you were being bullied. You are responsible for your own behaviour - so don't distress other people or encourage others to do so.

If you are being bullied

It is never your fault. It can be stopped and it can usually be traced.

- Don't ignore the bullying. Don't reply, but do tell someone you can trust, such as a teacher or parent, or call an advice line.

- Try to keep calm. If you seem frightened or angry it will only make the person bullying you more likely to continue.

Text / video messaging

- You can turn off incoming messages for a couple of days.
- If bullying persists you can change your number (ask your mobile phone provider).
- Do not reply to abusive or worrying messages. You can report them to your mobile phone provider.

Email

- Never reply to unpleasant or unwanted messages.
- Don't accept emails or open files from people you don't know.
- Don't delete bullying emails – print them or save them as evidence in a separate folder.

Social networking sites, chatrooms and instant messaging

- Change privacy settings so you can choose who to be friends with and who can see your profile. Don't add anyone you don't know to your friend list.
- Don't use your real name in chatrooms.
- Never give out your photo or personal details, like your address, phone number or which school you attend.
- Don't post any pictures or videos you wouldn't be happy for your parents or teachers to see. Once they are online, they can be copied and posted in other places where you can't get rid of them.
- Keep your passwords private and don't tell anyone, not even your best friend.

To report suspicious behaviour online and to learn more about keeping yourself safe online, visit www.thinkyouknow.co.uk

Always report bullying incidents. Not doing that allows the bully to continue. That's not good for the victims, for those who witness the incidents or for the bully, who may need help to change their anti-social behaviour.

Remote Learning

As every child starts at St Mary's CE Primary School, we provide them with a Google account. This means that they are able to access a range of resources from Google, including Google Docs, Classrooms, Gmail and Google Meet to help with their learning throughout their time here. In addition, we use this platform for home learning (and remote learning if necessary) (see the Remote Learning Policy)

To activate this, follow these simple steps

1. Search for Google.co.uk

2. Click on the sign in button in the top right-hand corner.
3. Sign in with the email address given by the class teacher.
4. Then input the password
5. Once in, click on the 9 dots in the right-hand corner. Here you will find access to all Google services.

Using Google allows pupils access to Gmail (emails). To increase our children's safety while they are online, we have blocked students from sending and receiving emails to accounts that are not @pupil.stmarysprimarypulborough.co.uk. They are also blocked from being able to access Google Chat.

The school has access to all students' accounts and can block students' access if children do not act appropriately. With that in mind, please could you talk with your child about the importance of not using their new email address for any other use apart from logging onto Google. In addition, it is vital that they do not share their username or password with others. In this way we can ensure that we are doing our utmost to keep our children safe online.

Key Stage 1 and 2