St. Mary's Church of England Primary School Fownhope

POLICY FOR E-SAFETY

Walking together in the fruit of the Spirit

UPDATED APRIL 2026

A rich education is more than simply learning reading, writing and maths. It is about helping a child grow into their full potential as inquisitive, well balanced and cheerful adults. As a Christian school we nurture children to display the 'fruit of the Spirit', which is "love, joy, peace, patience, kindness, goodness, faithfulness, gentleness and self-control" (Galatians 5:22-23). At St Mary's you will find children growing in mind, body and spirit as they form good relationships with each other, the staff and discover a faith which will sustain them in a rapidly changing world.

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, at St Mary's we need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

E-safety involves pupils, staff, governors and parents making best use of technology, information, training and this policy to create and maintain a safe online and ICT environment for St Mary's 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 possibly illegal.
"To ignore e-safety issues when implementing the requirements of Every Child Matters could ultimately lead to significant gaps in child protection policies, leaving children and young people vulnerable."
From: Safeguarding Children in a Digital World. BECTA 2006

Our e-safety Policy has been written by the school, following government guidance. It has been agreed and approved by governors.

- The school's e-safety coordinators are Mr Milne and Miss Scrivens
- The e-safety Policy and its implementation shall be reviewed biennially.

Roles and Responsibilities

Governors:
Governors are responsible for the approval of the e-Safety Policy and for reviewing the effectiveness of the policy. The role of the E-Safety Governor will include:

- Regular meetings with the e-Safety Co-ordinator/Officer
- Regular monitoring of e-safety incident logs
- Reporting to the Behaviour & Safety Committee.

Headteacher:
- The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the e-Safety Co-ordinator.
- The Headteacher is responsible for ensuring that the e-safety Coordinator and other relevant staff receive suitable training and professional development to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Headteacher should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The E-Safety Co-ordinator:

- Takes day-to day-responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policy/documents.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Provides training and advice for staff.
- Liaises with school ICT technical staff.
- Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.

Teaching and Learning
The Internet is an essential element for education, business and social interaction. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality Internet access as part of their learning experience:

- Children will be supervised by adults when using the Internet in school.
- The school Internet access will be designed expressly for pupil use including appropriate content filtering.
- Pupils will be given clear objectives for Internet use and taught what use is acceptable and what is not.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- As part of the new ICT (computing) curriculum, all year groups have digital literacy units that focus on different elements of staying safe online. These units include topics from how to use a search engine, digital footprints and cyber bullying.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.

Through ICT we ensure that the school meets the needs of all, taking account of gender, ethnicity, culture, religion, language, sexual orientation, age, ability, disability and social circumstances. It is important that we meet the diverse needs of pupils to ensure inclusion for all. We also measure and assess the impact regularly through meetings our SEN co-ordinator and individual teachers to ensure all children have equal access to succeeding in this subject.

Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of information

World Wide Web

The Internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- If staff or pupils discover unsuitable sites, the URL (address), time and content shall be reported to the teacher who will then report to the Headteacher, by recording the incident in an e-Safety Log, which will be stored in the Headteacher's office with other safeguarding materials. The e-Safety Log will be reviewed termly by the e-Safety Co-ordinator.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- The school will work in partnership with the Local Authority and our IT consultants to ensure that filtering systems are as effective as possible.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

Social Networking

This policy should be read in conjunction with the school's 'Social Media and Mobile Phone Policy'. The key points are listed below.

- Pupils are not allowed to access Social Media sites in school. Staff may only access such sites during recognized breaks, and only in the staffroom. Staff are discouraged from accessing Social Media sites whilst on school premises.
- Staff must never add pupils (including ex-pupils still under 16) as 'friends'.
- Staff must not post comments about the school, pupils or parents on Social Media. Staff must not post information or opinions about St Mary's.
- Parents must not post pictures of children (other than their own) taken at school events, or identify school staff on Social Media sites.

During ICT lessons (and PSHE lessons) pupils will regularly be reminded of the importance of internet safety. Whilst most Social Networking sites have a minimum age requirement that should preclude St Mary's pupils from joining, the school appreciates that this isn't always the case. Therefore, the following points will be strongly reinforced:

- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location. This will also include not using personal photographs and videos.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Pupils will be encouraged to only interact with known friends and family over the Internet and deny access to others.

Reporting

All breaches of the e-safety policy need to be recorded in the E-Safety reporting book that is kept in the school office. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to one of the school's Designated Safeguarding Leads immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues but may require intervention (e.g. cyberbullying) should be reported to the Headteacher on the same day.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (e.g. Ceop button, trusted adult, Childline)

Mobile Phones and Digital Photography

Children are not allowed to have mobile phones in school. If children bring a phone to school they should take it to the school office where it will be kept until the end of the school day.

Pupils at St Mary's CE Primary School have their photograph taken in order to provide evidence of their achievements for their developmental records.

A current, up to date list of those pupils whose parents / carers have refused permission for them to be photographed is kept in the school office and is accessible to all staff.

Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of school children for their own records during the school day.

Procedures

- Under the data protection act of 1998 school must seek parental consent to take photographs and use video recorders. Photographs will be stored on the school network which is password protected until the school ceases to operate, should this occur then all photographs will be shredded or deleted from the school network.
- The school's digital cameras must not leave the school setting (unless on an educational visit).
- Photographs are printed in the setting by staff and images are then removed from the camera memory.
- Photographs of children may be taken and used in accordance with parental consent obtained via the Media Permission Form.
- Only photographs containing children whose parents have given their consent may be placed on the school website or given to third parties.
- Often photographs may contain other children in the background.
- Events such as Sports Day, outings, Christmas and fundraising events may be photographed and/or recorded on video by staff, but always in full view of all attending. These images must be stored on secure school files only.
- Parents must not post photographs or video containing other children on social media websites. (See Policy above).
- Many mobile phones have inbuilt cameras so staff mobile phones must not be used to take pictures of children in our school.
- **Visitors may only use their phones outside the building and should be challenged if seen using a camera inappropriately or photographing children.**
- The use of cameras and mobile phones are prohibited in toilets.
- The school appreciates that staff occasionally need to make personal calls during school hours. However, these should be kept to a minimum. Excessive making, or receiving, of personal calls could lead to disciplinary action.
- All school cameras, iPads and other image recording devices should be kept securely at all times and used with appropriate authority.

To protect children we will:

Within the school:

- seek their consent for photographs to be taken or published (for example, on our website or in newspapers or publications)
- seek parental / carer consent for images of their children to be used. If consent is not given no images of that child will be used. An up-to-date list of those children whose image cannot be used is easily accessible via the office
- use only the child's first name with an image

- ensure that children are appropriately dressed
- encourage children to tell us if they are worried about any photographs that are taken of them.

When off site, in a controlled environment:-

- Ask those people involved to guarantee that any photographs taken will not be used on any social media site, explaining the reasons why. Lead staff must ensure that this is done.
- Alternatively, if possible gain written permission from parents before the visit for children for images of their child to be posted on social media sites. It is the lead member of staff's responsibility to ensure that only photographs containing children whose parents have given their written permission are posted onto social media sites.

When pupils are visiting an uncontrolled site:-

- Where the school cannot guarantee that photographs will not be taken and posted onto social media sites (e.g. at a football match), parents will be notified of this before the visit. If a parent is then concerned about their child's photograph being exposed on a social media site, then that parent should request that their child does not participate in the event.

Sexting (Youth Produced Sexual Imagery)

Unfortunately, as mobile phones, tablets and other devices become more ubiquitous, there is an increased chance of inappropriate pictures / videos or text messages being produced and sent by pupils. As the guidance in the UK Council For Child Internet Safety's document 'Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People' (SiSaC) explains, the laws around 'sexting' are complex. This is particularly true with regard to written messages, and the guidance in this policy is therefore intended to cover the making and sending of images. In order to make this definition clearer, the SiSaC document replaces 'sexting' (a 'catch-all' term that is difficult to define) with the term 'Youth Produced Sexual Imagery'.

The sharing of sexual imagery of people under 18 by adults constitutes child sexual abuse. If the school becomes aware of any incidents of this it will **always** contact the police

The situation becomes more complex when a person under the age of 18 creates or shares sexual imagery. In law this is illegal, even if the image of a person under 18 has been created by themselves. If the school becomes aware of any such images it will always treat the matter as a safeguarding incident and, unless there are exceptional circumstances, contact the parents / carers of the children involved. However, as the SiSaC document states,

> *The law criminalising indecent images of children was created long before mass adoption of the internet, mobiles and digital photography. It was also created to protect children and young people from adults seeking to sexually abuse them or gain pleasure from their sexual abuse.* ***It was not intended to criminalise children***

The school will therefore use its discretion as to whether to involve outside agencies or keep the matter within school.

Published Content and the School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the Website will be the school address, e-mail and telephone number.
- Staff and pupils' personal information will not be published.

- Either the Headteacher or a nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and pupils' full names will not be used in association with photographs.
- Consent from parents will be obtained before photographs of pupils are published on the school website.
- Work will only be published with the permission of the pupil.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.
- E-safety will be discussed with our ICT support and those arrangements incorporated into our agreement with them.

Protecting Personal Data
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act

Assessing Risk

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. The school does not accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Handling E-Safety Complaints

- Complaints of Internet misuse will be dealt with by the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be referred to the Designated Safeguarding Lead (or Deputy DSL) and shall be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the community police officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils:

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be informed of the importance of being safe on social networking sites.

Staff:

- All staff will be expected to have read the school's 'E-safety Policy' and 'Social Media and Mobile Phone Policy' and understand their importance.

Parents:

- Parents' attention will be drawn to the school's 'E-safety Policy' and 'Social Media and Mobile Phone Policy' in newsletters and on the school website.

In line with the school's guidelines this policy will be reviewed annually.

This policy was approved by the Governing Body in:	April 2026
Signature of Headteacher:	T. Milne
Signature of Chair of Governors:	A. Gunn
Review Date:	April 2027