Learning to love
Loving to learn

ST MARY'S CE (A) FIRST SCHOOL
MOBILE PHONE, DIGITAL TECHNOLOGY & AI POLICY

"Our Vision is to provide the best opportunities to become life-long learners.
Our Christian values rooted in the Good Samaritan recognise everyone is loved by God.
Our ethos is to show love and respect – to ourselves, each other and God's creation"

Intent

In order for the governors of St Mary's First School to ensure the safety of all who attend or work in the school they have set the guidelines below. This document is linked to the school's Early Years Foundation Stage Policy, the Safeguarding Policy, the Code of Conduct and the Online Safety policy.

Aims

To ensure the safety of children, staff, governors, students and volunteers

Guidelines

- Staff, governors and volunteers should not use mobile phones or smart devices to receive or make phone calls, texts or emails, or to access the internet in school when working with or in the vicinity of children.
- Personal phones should be switched to silent mode and in a secure place, which cannot be accessed by pupils.
- Adults wearing smart watches should ensure they are not receiving or sending messages whilst supervising children in the classroom.
- Personal phone calls should only be made during break times or before or after school.
- Incoming calls should be on answer phone and accessed as above.
- In the case of emergencies, incoming calls should be made to the school office on 01889 228730 and these will be relayed by a member of staff and, if immediate response is required, arrangements to oversee children will be made.
- Mobile phone cameras must not be used to take photographs of children. School ipads or school memory cards, for use in personal cameras, are provided to record activities for assessment purposes or for evidence of activities or performances.
- School memory cards, for use in personal cameras, must be signed in and out by the member of staff if they are taken off site.
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents comment on any activities involving other pupils in the digital or video images.
- Staff and volunteers are allowed to take digital or video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, as outlined above.
- Care should be taken when taking digital or video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or school facebook pages.
- Pupil's work can only be published with the permission of the pupil and parents or carers.
- Staff must ensure that they take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they "log-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

- When personal data is stored on any portable computer system, memory stick or any other removable media:
  * The data must be encrypted and password protected.
  * The device must be password protected eg memory stick, hard drive.
  * The device must offer approved virus and malware checking software.
  * The data must be securely deleted from the device once it is transferred.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data eg assessment information can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.

The only exception to these guidelines is when staff use their mobile phones for emergency contact when they are out of the classroom environment e.g. on the school field or on a school trip.
Staff in the lower building may need to use a phone for emergency contact to the school office if access to the landline is restricted. The option of using walkie-talkies is available, and staff are aware to keep communication minimal and restricted, with awareness of GDPR.

Many children now have unlimited and unrestricted access to the internet via mobile phone networks at home. The breadth of issues classified within online safety on mobile devices is considerable and ever evolving, but can be categorised into four areas of risk:
content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images. e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams.

If we feel our pupils, students or staff are at risk, we will report it to the Anti-Phishing Working Group.
https://apwg.org/

The Use of AI in school

This section outlines the school's expectations, safeguards, and principles for the safe, ethical, and age-appropriate use of Artificial Intelligence (AI) within the primary school setting. AI tools include educational platforms that use adaptive learning, automated feedback, generative AI, and other intelligent technologies.
Our aim is to ensure AI supports teaching and learning while protecting pupils' safety, privacy, and wellbeing.
St Mary's First School will ensure that AI use is:

- **Age-appropriate**: Any AI tool used with pupils must be suitable for the age of the children and aligned with the curriculum.
- **Safe and secure**: Tools must comply with data protection legislation and safeguarding requirements.
- **Transparent**: Staff, parents, and pupils should understand when and how AI is being used.
- **Teacher-led**: AI must support teachers, not replace professional judgement.
- **Ethical**: AI use must be fair, unbiased, and respectful of pupil rights.

AI may be used in school for:

- Adaptive learning systems that tailor content to pupil needs.
- Automated feedback on spelling, grammar, numeracy, or practice tasks.
- Teacher planning, resource creation, or administrative support.
- Accessibility tools (speech-to-text, translation, predictive text) where appropriate.

AI must not be used for:

- Decision-making that affects pupil welfare or academic outcomes without teacher oversight.
- Emotional analysis, biometric data processing, or surveillance.
- Chat-based generative AI tools accessed directly by pupils unless part of a controlled, age-appropriate platform.

Data Protection and Privacy

Before any AI tool is introduced, the school will:

- Conduct a Data Protection Impact Assessment (DPIA) where required.
- Ensure the provider complies with the Data Protection Act and the Data (Use and Access) Act 2025.
- Verify that only the minimum necessary pupil data is shared.

Pupils' personal data must never be entered into public AI tools

Staff must:

- Use only AI tools approved by the school.
- Ensure AI-generated content is checked for accuracy and appropriateness.
- Avoid sharing sensitive information with AI systems.
- Report any concerns or misuse immediately to the Digital Lead or DPO.
- Complete AI-specific training as provided by the school.

Pupil Use of AI:

- AI use by pupils will be supervised and limited to approved educational platforms.
- Pupils will not use open-ended AI chat tools unless part of a curated, school-approved activity.
- Pupils will be taught how to use AI responsibly, including understanding that AI can make mistakes, the importance of online safety and how to recognise unreliable content.

The school will inform parents when AI plays a significant role in a learning tool or platform. Parents will be given clear information about what the tool does, what data it uses and how data is protected.

Monitoring, Review, and Compliance

The school will:

- Regularly review the use of AI tools to ensure they remain safe, effective, and appropriate.
- Remove or replace any AI resources that no longer meet required standards.
- Update this section in line with emerging guidance from the Department for Education and the Information Commissioner's Office.
- Conduct annual AI risk assessments for all approved AI tools.
- Maintain records of staff training, pupil guidance, and parental communications.

AI Risk Assessment Checklist:

Before implementing any AI tool, staff must check:

1. **Educational purpose:** Does it align with curriculum objectives?
2. **Age-appropriateness:** Is the content suitable for primary pupils?
3. **Data protection compliance:** Does the tool minimise data sharing and comply with legislation?
4. **Safeguarding:** Are there risks of exposure to inappropriate content?
5. **Bias and ethics:** Are outputs free from harmful bias?
6. **Teacher oversight:** Can the tool be monitored by staff at all times?
7. **Training:** Have staff completed AI-specific training?

Monitoring

Head Teacher, Senior Management and Governing Body
Agreed by Staff and Governing Body November 2025.
Review: November 2027