



**ST MARY'S CofE
PRIMARY SCHOOL**



St Mary's C of E Primary School Online Safety Policy

including Prevent and statutory
requirements for Sex and Relationship
Education

Reviewed April 2026

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers and visitors who have access to and are users of school ICT systems, both in and out of the school.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school Online Safety Policy and practices
- they understand their obligations under the Keeping Children Safe in Education statutory guidance
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problems to the Headteacher or SENCO for investigation.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- they monitor the use of digital technologies in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- they recognise the warning signs of children at risk of radicalisation or extremism and report in line with Prevent Duty (1st July 2015)
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Resources for teaching E-Safety

- National Online Safety
- Purple Mash
- KidSmart <http://www.kidsmart.org.uk/>
- BBC Stay safe <http://www.bbc.co.uk/cbbc/help/web/staysafe>
- Be internet awesome by Google
- Think U Know from NCA/CEOP <https://www.thinkuknow.co.uk/>
- Picture News

Pupils

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website
- their children's personal devices in the school (where this is allowed)

Policy Statements

Education – Pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating *pupils* to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and lessons
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school.
- Staff should act as good role models in their use of digital technologies the internet and mobile devices

Pupils will be taught the following as part of our e-safety program:

How to evaluate what they see online - This will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.

- Pupils will be asked to consider questions including:
 - is this website/URL/email fake? How can I tell?
 - what does this cookie do and what information am I sharing?
 - is this person who they say they are?
 - why does someone want me to see this?
 - why does someone want me to send this?
 - why would someone want me to believe this?
 - why does this person want my personal information?
 - what's behind this post?
 - is this too good to be true?
 - is this fact or opinion?

How to recognise techniques used for persuasion – This will enable pupils to recognise the techniques that are often used to persuade or manipulate others. Understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to strongly biased intent or malicious activity.

- Children will be supported to recognise:
 - online content which tries to make people believe something false is true and/or mislead (misinformation and disinformation),
 - techniques that companies use to persuade people to buy something, 7 ways in which games and social media companies try to keep users online longer (persuasive/sticky design); and criminal activities such as grooming.

Online behaviour – This will enable pupils to understand what acceptable and unacceptable online behaviour look like. We will teach pupils that the same standard of behaviour and honesty apply on and offline, including the importance of respect for others. We will also teach pupils to recognise unacceptable behaviour in others.

- We will help pupils to recognise acceptable and unacceptable behaviour by:
 - looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do,
 - looking at how online emotions can be intensified resulting in mob mentality, (how people can be influenced by their peers to adopt certain behaviours on a largely emotional, rather than rational, basis)
 - teaching techniques (relevant on and offline) to defuse or calm arguments, for example a disagreement with friends, and disengage from unwanted contact or content online; and

- considering unacceptable online behaviours often passed off as so-called social norms or just banter. For example, negative language that can be used, and in some cases is often expected, as part of online gaming and the acceptance of misogynistic, homophobic and racist language that would never be tolerated offline.

How to identify online risks – This will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.

We will help pupils to identify and manage risk by:

- discussing the ways in which someone may put themselves at risk online,
- discussing risks posed by another person's online behaviour,
- discussing when risk taking can be positive and negative,
- discussing "online reputation" and the positive and negative aspects of an online digital footprint. This could include longer-term considerations, i.e. how past online behaviours could impact on their future, when applying for a place at university or a job for example,
- discussing the risks vs the benefits of sharing information online and how to make a judgement about when and how to share and who to share with; and
- asking questions such as what might happen if I post something online? Who will see it? Who might they send it to?

How and when to seek support – This will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.

We will help pupils by:

- helping them to identify who trusted adults are,
- looking at the different ways to access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation. This links to wider school policies and processes around reporting of Safeguarding and child protection incidents and concerns to school staff (see Keeping Children Safe in Education); and
- helping them to understand that various platforms and apps will have ways in which inappropriate contact or content can be reported.

Who to talk to should they need support – This will enable children to know who is available to support the children should they need it:

- Childline for free and confidential advice

- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Children to be aware of online safety which can be classified 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 – personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending or receiving explicit images (e.g. consensual and non-consensual 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.

Education – Parents / Carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on- line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters and the website
- Parents / Carers evenings
- High profile events / campaigns e.g. Safer Internet Day

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Agreements.
- Participation in school / academy training / information sessions for staff or parents
- Staff to be trained to identify behaviour that causes concern that the child is at risk of radicalisation or extremism.

Technical – infrastructure / equipment, filtering and monitoring

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

- There will be regular reviews and audits of the safety and security of school technical systems
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by the IT Co-Ordinator who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password
- Internet filtering should ensure that children are safe from terrorist and extremist material when accessing the internet
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.
- Filtering and monitoring will ensure that children are kept safe from terrorist and extremist material when accessing the internet in school in line with current guidance of the Prevent Duty (1st July 2015)

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press
- Staff and volunteers are allowed to take digital / 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, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / 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.

Pupil Acceptable Use Agreement KS1

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computing equipment in school (this includes laptops and iPads).
- I will only use websites, applications (apps) and software that a teacher or suitable adult has told or allowed me to use.
- I will follow all instructions given to me by a teacher or responsible adult.
- I will take care of the computing equipment so that it is available for others to use.
- I will ask for help from a teacher or suitable adult if I am not sure what to do.
- I will ask for help from a teacher or suitable adult if I think that there is something wrong or I have accessed something by mistake.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I will treat everyone fairly and with respect when communicating with them online
- I understand that people I do not know are strangers on the internet and I must not share my own, or anybody else's, personal information (this includes names, date of birth, email, address, school name).
- I will keep all passwords safe and not share them with anyone else.
- I know that if I break the rules I may not be allowed to use the computer equipment and if necessary further action may be taken.

Pupil Acceptable Use Agreement KS2

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computing equipment in school (this includes laptops and iPads).
- I will only use websites, applications (apps) and software that a teacher or suitable adult has told or allowed me to use.
- I will follow all instructions given to me by a teacher or responsible adult.
- I will take care of the computing equipment so that it is available for others to use.
- I will ask for help from a teacher or suitable adult if I am not sure what to do.
- I will ask for help from a teacher or suitable adult if I think that there is something wrong or I have accessed something by mistake.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I will treat everyone fairly and with respect when communicating with them online and understand that cyberbullying is not acceptable.
- I understand that people I do not know are strangers on the internet and I must not share my own, or anybody else's, personal information (this includes names, date of birth, email, address, school name).
- I will keep all passwords safe and not share them with anyone else.

- I understand that the use of computers in school is digitally monitored and any attempts to access websites, software or applications will be reported.
- I understand that I must only download digital content that I have permission to use – this includes pictures and videos from websites.
- I know that if I break the rules I may not be allowed to use the computer equipment and if necessary further action may be taken.