



Martley C.E. Primary School

Online Safety Policy

Document Full Name	Online Safety Policy
Developer/Developer's Role	David Prince (Computing Subject Lead)
Edition Date	September 2024
Approval Responsibility	LAB
Review Cycle	Annually
Next Review Date	September 2025

Our Christian Values

Our Core Christian values are the 5 C's - Commitment, Creativity, Compassion, Co-operation and Courage. They permeate our curriculum and are taught through our collective worship, within our curriculum and as part of our personal development programme.

Our vision is that everyone will know that they are loved by God. We nurture all children and adults so that they flourish as individuals and make the best of their God-given talents, through embracing our diverse world.

'Every good action and every perfect gift is from God. These good gifts come down from the creator of the sun, moon and stars. God does not change like their shifting shadows'.

James 1:17 International Children's Bible

We also support and follow the vision of the Diocese of Worcester Multi-Academy Trust (DoWMAT) of which we are a member school:

'To Love, To Learn, To Serve' sums up the DoWMAT's vision for those who come together to create the MAT, enabling all to flourish both as individuals and in community with each other; living life in all its fullness (John 10:10).

Equality and Diversity Statement

At Martley CE Primary School and Pre-School we promote equality of opportunity. We promote positive attitudes and encourage active participation of all stakeholders regardless of race, gender, disability, age, religion, belief and sexuality.

In so doing we strive to eliminate any unlawful discrimination or harassment of any group and where any such harassment is found appropriate action will be taken immediately.

Aims

At Martley CE Primary School, we aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as 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, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and seminudes and/or pornography), sharing other explicit images and online bullying

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education

(https://assets.publishing.service.gov.uk/media/6650a1967b792fff71a83e8/Keeping_children_safe_in_education_2024.pdf), and its advice for schools on:

- Teaching online safety in schools (<https://www.gov.uk/government/publications/teaching-online-safety-in-schools/teaching-online-safety-in-schools>)
- Preventing and tackling bullying, cyber-bullying and advice for headteachers and school staff
- Relationships and sex education

It also refers to the DfE's guidance on protecting children from radicalisation

(<https://www.gov.uk/government/publications/the-prevent-duty-safeguarding-learners-vulnerable-to-radicalisation>).

It reflects existing legislation, including but not limited to the Education Act 1996 the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum programmes of study.

Roles and responsibilities

Local Academy Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures

Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

The Headteacher

The Headteacher responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incident
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher and/or Local Academy Board

The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

All Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood, and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre (<https://saferinternet.org.uk/>)

- Hot topics – Childnet International (<https://www.childnet.com/>)
- Parent resource sheet – Childnet International

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools (<https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education/relationships-education-primary>)
- Relationships and sex education and health education in secondary schools (<https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education/relationships-and-sex-education-rse-secondary>)

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact By the end of primary school, pupils will know:
 - That people sometimes behave differently online, including by pretending to be someone they are not
 - That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
 - The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
 - How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
 - How information and data is shared and used online
 - What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
 - How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Educating Parents about Online Safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

Cyber Bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation (https://assets.publishing.service.gov.uk/media/62d1643e8fa8f50bfef55c/Searching_Screening_and_Confiscation_guidance_July_2022.pdf) and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people (<https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis#ukccis-publications>)

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation (https://assets.publishing.service.gov.uk/media/62d1643e8fa8f50bfefa55c/Searching_Screening_and_Confiscation_guidance_July_2022.pdf)
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people (<https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis#ukccis-publications>)

Our Behaviour Policy / Searches and Confiscation Policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. Martley CE Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Martley CE Primary School will treat any use of AI to bully pupils in line with our behaviour policy. Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Acceptable Use of the Internet in School

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Staff Using Work Devices Outside of School

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password protected
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the DSL

How the School will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in relevant policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
 - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices

and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the Computing Lead and Headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.



Martley C.E. Primary School

Acceptable Use Agreement (EYFS/KS1)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Ask a teacher or adult if I can do so before using them
- Only use websites that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
 - I click on a website by mistake
 - I receive messages from people I don't know
 - I find anything that may upset or harm me or my friends
- Use school computers for school work only
- Be kind to others and not upset or be rude to them
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
- Save my work on the school network
- Check with my teacher before I print anything
- Log off or shut down a computer when I have finished using it

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.

Signed (parent/carer):

Date:



Martley C.E. Primary School

Acceptable Use Agreement (KS2)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

Name of pupil:

I will read and follow the rules in the acceptable use agreement policy.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Signed (pupil):

Date:

Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date:



Martley C.E. Primary School Acceptable Use Agreement (Staff)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's
 - network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

- I will only use the school's ICT systems and access the internet in school, or outside school on a work device,
- for educational purposes or for the purpose of fulfilling the duties of my role.
- I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
- I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
- I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date: