St Mary's C of E Primary School

Internet Safety Policy

2024-2025

St Mary's C of E Primary

Name of Policy: Internet Safety Policy

Author: Carol Benson

Adopted following governor approval: June 2024

Review date: June 2025

This school is committed to safeguarding and promoting the wellbeing of all children, and expects our staff and volunteers to share this commitment. Please report any safeguarding or child protection concerns to the designated teachers for Child Protection:
Mrs Benson, Mrs Whitehead & Mr Butterwick

The Governors and Staff of St Mary's CE Primary School are committed to educating the children spiritually, academically, emotionally and physically within a distinctive Christian ethos.

"Through God we live and learn"

'The fruit of the spirit is love, joy, peace, patience, kindness, goodness, faithfulness, gentleness, self-control; against such things there is no law' (Galatians 5:22)

Love, respect and moral understanding lie at the heart of the ethos of St Mary's Church of England Primary School. We see our learners as the future custodians of God's world. We aim to nurture and encourage happy individuals who are socially engaged and curious about life within and beyond their own community. We value and encourage difference and diversity. St Mary's is a nurturing, safe place for children to question, to learn to love and respect other people and to discover their place in the world. We have traditional values, rooted in the Christian faith, as well as global, 21st Century aspirations for all our pupils.

St Mary's is part of the Wharfe Valley Learning Partnership, a collaborative of schools in Wetherby and Boston Spa, where the vision for all children is to be respectful, globally aware and compassionate as well as ambitious, resilient and engaged in their learning.

Introduction

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. The Internet Safety Policy is designed to ensure safe and appropriate use.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Identify and support groups of pupils that are potentially at greater risk of harm online than others.
- 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 and smart 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 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.

Scope of this policy

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

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other internet safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate internet safety behaviour that take place out of school.

Roles and Responsibilities

The governing board

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

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

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

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and regularly review their effectiveness.

The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

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

The designated safeguarding lead and or headteacher

Details of the school's designated safeguarding leads (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 and governing board to review this policy annually and ensure

the procedures and implementation are updated and reviewed regularly.

- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
- Working with the ICT manager to make sure the appropriate systems and processes are in place.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's 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 safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing board.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.
- Will keep a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.

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.
- Knowing that the DSL / headteacher is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents.
- Following the correct procedures by speaking to the headteacher if they need to bypass the filtering and monitoring systems for educational purposes
- 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'

This list is not intended to be exhaustive.

Parents/carers

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

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Educating pupils about online safety

In Key Stage (KS) 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 (KS) 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

Following COVID-19, each pupil from Year 2 onwards has an Office 365 account. At present, children are able to use the provided email accounts, however, can only email people within the school group (Staff and other pupils.)

Internet use will enhance learning

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries.
- Inclusion in government initiatives.
- Educational and cultural exchanges between pupils world-wide.
- Access to experts in many fields for pupils and staff.
- Development of a more effective form of interschool communication.
- Staff professional development through access to national initiatives.
- Educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.

Pupils will be taught what Internet use is acceptable and what is not, and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Educating parents/carers about online safety

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

The school will let parents/carers 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

If parents/carers 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.

Concerns or queries about this policy can be raised with 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. (See also the school behaviour policy.)

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/carers as part of our #WakeUpWednesday initiative so 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 headteacher 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 Chair of Governors.
- 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 staff members or pupil's co-operation

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 headteacher, in consultation with the Chair of Governors, 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 headteacher and chair of governors 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/carer 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 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
- Any searching of pupils will be carried out in line with:
- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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. St Mary's C of E 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.

St Mary's C of E 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.

Filtering & Monitoring

Filtering and monitoring will be in line with KCSIE 2023 guidance.

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

The uses EXA Networks (Surf protect Quantum) to ensure systems to protect pupils are in place, reviewed and improved.

If staff or pupils discover an unsuitable site, it must be reported to the Internet Safety Officer and logged immediately using the school's Computing Incident Report Log.

The internet safety officer will, upon a site being reported, log on to Surf protect and block the reported website.

Surfprotect sends a daily incident log to schools finance mailbox at 15:30 each day. The school office prints this report and adds it to the filtering and monitoring file.

Surfprotect sends the school finance mailbox immediate incident reports as soon as access to inappropriate / blocked content is requested. These are printed by the school office and investigated.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by the e-safety coordinator Oliver Butterwick, and a senior member of staff.
- Any complaint about staff misuse must be referred to the head teacher, Carol Benson.
- Complaints of a child protection nature must 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 Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Wireless Network

- The schools wireless network is secure. There is a password which only Vital (the Provider) knows.
- Pupil devices (iPads and chrome books provided by school) are already set up on the network.
- Staff are advised to contact the computing leader when accessing with personal equipment.
- It will be managed by the computing subject leader

E-mail

- Following COVID-19, each pupil from Year 2 onwards has an Office 365 account. At present, children are able to use the provided email accounts, however, can only email people within the school group (Staff and other pupils.)
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and content should be professional in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The headteacher, Carol Benson, Oliver Butterwick(Computing leader) and Hannah Thomas

(Business Manager) take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Only pupils' forenames will be used on the Web site, especially in association with photographs.
- Pupil's work can only be published with the permission of the parents (List of non-authorised children has been created for every year group).
- All parents / carers will need to give consent before their child(ren)s photographs or videos will appear on the website.

Social Media

Social media applications (such as Facebook and Twitter; instant messaging and file-sharing 'apps' on mobile devices; blogging websites; discussion forums) bring opportunities for children, young people and adults to understand, engage and communicate with audiences in new and exciting ways. It is important that we are all able to use these appropriately and safely.

All children at St. Mary's Church of England Primary School have opportunities to access the Internet in a safe and supervised environment, when on-site. They are not permitted to access Facebook. We sincerely hope that no child can access Facebook outside of school, as those under the age of 13 should not be registered as users.

Staff are expected to follow the rules laid out in the staff code of conduct in regards to social media accounts, failure to do so could result in disciplinary action.

We aim to:

- Balance the schools support for innovation whilst providing a framework for best practice.
- Ensure the school is not exposed to safeguarding or legal risks.
- Ensure that the school's excellent reputation is not compromised.
- Ensure that users of social media applications are able to clearly distinguish where information provided via social media is legitimately representative of the school.
- Ensure that staff, governors and members of the schools wider community understand the rules and regulations surrounding social media in school.

All users of social media applications should bear in mind that the information they share, even if on private 'spaces', is still subject to copyright, data protection and Freedom of Information legislation, as well as the Safeguarding Vulnerable Groups Act of 2006.

Social networking applications must not be used by employees for personal use, during working hours, unless the express permission of the Head teacher is obtained.

Any proposed use of social networking applications as part of a school service/activity (whether they are hosted by the school or by a 3rd party) must be approved by the Head teacher first.

School users must adhere to the following Terms of Use:

Social media applications:

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages; this includes, but is not limited to, material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Must not be used for the promotion of financial interests, commercial ventures that result from your association with school or personal campaigns that may affect the reputation of school.
- Must not be used in an abusive or hateful manner.
- Must not be used for actions that would put the employees, Governors or children in breach of school codes of conduct or policies.

- Must not breach the school's Disciplinary Policy, Equality Policy, Anti-bullying Policy and Confidentiality Policy.
- Must not be used to discuss or advise any matters relating to school issues, colleagues, children or parents.
- Must not facilitate online information-sharing 'friendships' with minors.
- Must not identify users as a representative of the school e.g. by using full names.
- Must not make reference to any employee, child, parent or school activity or event unless prior permission has been obtained from the Head Teacher.
- Must not be used to share out-of-work activities, which may cause embarrassment to the employer or detrimentally affects the employer's reputation. This will result in disciplinary action.
- Must not be used by children in an attempt to access a school employee or Governor's area or 'space' on a network.

School staff, governors and members of the wider school community should be aware that nothing posted on social media sites is truly secure and it could, therefore, fall under the scrutiny of school and the wider community.
Members of any individual's social media network could easily take screen shots of anything posted on social media and share these with others.

Monitoring of this policy

Any violation of this policy will be considered as potentially gross misconduct under the school's Disciplinary Policy (Staff); under the Code of Conduct (Governors) and under the school's Behaviour and Exclusion Policies (Children).

All employees, Governors and children are encouraged to report any suspicions of the misuse of social media applications to the Head Teacher or trusted adult. If the Head Teacher receives a disclosure that an adult employed by the school is using social networking in an inappropriate way as detailed previously, this should be recorded in line with the Child Protection Policy and/or Disciplinary Policy.

Children are strongly encouraged to report to a trusted adult any worries they have about cyberbullying or improper contact. The school has a duty of care to investigate and work with children and families where there are reports of cyberbullying/misuse of social media applications out of school hours.

This policy will be reviewed every year by the headteacher. At every review, the policy will be shared with the governing board. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Related School Documents & Policies

KCSIE Sept 2023
Complaints Policy
Staff Code of Conduct
Data Protection Policy
Internet Acceptable Use Agreement
ICT & Computing Policy
Anti-Bullying Policy
Child Protection Policy Staff Disciplinary Policy

Policy Review

This policy will be reviewed every year or sooner if deemed necessary.

Pupil Acceptable Computer Use Agreement / Internet Safety Rules

Dear Parent/Carer

As part of pupils' curriculum enhancement and the development of Computing skills, we provide supervised access to the Internet in school.

School issues pupils with usernames and passwords for use online. In addition to this, computer use is supervised within the classroom.

However, there are risks involved in Internet use. Below is a list of the school's rules for 'Responsible Internet Use', in-line with the Internet Safety Policy. We ask that at a time convenient to you, you discuss the Rules with your child – and their importance – and return the completed slip to school.

- I will only access the Internet using my username and password.
- I will only use computers and devices in school for school purposes.
- I will only use my own email address.
- I will make sure that all Computing contact with other children and adults is responsible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will turn off my computer or device and tell my teacher or a trusted adult immediately.
- I will not send anything that could be considered unpleasant or nasty.
- I will not give out my own details such as my name, phone number or home address.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using Computing because I know that these rules are to keep me safe.
- I will only access my own file and not access other people's work.
- I know that my use of Computing can be checked and that my parent/carer contacted if a member of school staff is concerned about my safety.

Computing and access to the Internet is a valuable aid to learning and we want to ensure that it is used safely. If you have any questions, please don't hesitate to contact me. Internet Safety meetings for parents will be taking place periodically.

Yours sincerely,

Mrs Benson

Pupil Acceptable Computing Use Agreement / Internet Safety Rules

Name of child …… Class……

We have discussed this and my child agrees to follow the Internet Safety rules and to support the safe use of Computing at St. Mary's Church of England Primary School, Boston Spa.

Parent/Carer Signature …… Date……...