



St Mary's CE Primary School



“Nurturing Success”

Date Reviewed: May 23
Date Due for Review: May 25

Online Safety Policy

Introduction

At St Mary's, we are committed to nurturing every child (and every adult) as a unique individual to be the best that they can be, within a safe, friendly and welcoming community rooted in Christian values. Our vision is to provide an education of the highest quality through a rich, broad and balanced curriculum which focuses on the development of the whole person. We want children to develop as happy, confident and articulate individuals who will love learning throughout their lives.

Our online safety policy is shaped by our school vision and values of friendship, respect, trust, hope, wisdom and perseverance.

Our Online Policy links to other key school policies including our Behaviour Policy, Strategic Child Protection and Safeguarding Policy, SEND Policy and Equality Policy.

1. Introduction and Aims

Keeping children safe in education 2022: Statutory guidance for schools and colleges (Department for Education (DfE, 2022) states that it is essential that children are safeguarded from potentially harmful and inappropriate online material.

Online Safety encompasses the use of technology on a wide variety of devices. In school, it can involve the use of online pupil collaboration and publishing and sharing work online. Increasingly, pupil data, work and other information assets are being stored online via learning platforms or other storage facilities. Outside of school, the availability of online resources is much more wide-spread.

‘Teaching online safety in schools guidance: supporting schools to teach their pupils how to stay safe online, within new and existing school subjects’ (DfE, 2019) advises that the online world develops and changes at great speeds with new opportunities, challenges and risks appearing all the time therefore it is important to focus on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app.

Online safety enables us to provide safeguards and awareness for all users to control and enhance their online experiences. It is not just about the risks and how we avoid them; it is about ensuring everyone has the chance to develop a set of safe and responsible behaviours that will enable them to reduce the risks, whilst continuing to benefit from the opportunities.

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

This policy reflects the school's aims in relation to the teaching and learning of Online Safety. It sets out a framework within which teaching and non-teaching staff can operate. Additionally, the policy aims to raise awareness of safety issues associated with electronic communications with all members of our school community.

Legislation and guidance

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

- Teaching online safety in schools (June 2019)
- Behaviour in schools Advice for headteachers and school staff (September 2022)

This policy also needs to be read in conjunction with other St Mary's Church of England Primary School policies including the Anti-Bullying Policy; Behaviour Policy; Strategic Child Protection and Safeguarding Policy, Acceptable Use Policy, Staff Code of Conduct, Data Protection policies as well as the East Riding of Yorkshire Council policies and guidance for Use of the Internet and Use of Electronic mail (Email).

Our aims for online safety at St Mary's CE Primary school are that:

- there are agreed expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- stakeholders are aware of their responsibilities and understand how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world
- clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms are in place
- children are prepared to be safe and responsible users of online technologies

2. Roles and Responsibilities within Online Safety

All members of the school community have a duty to be aware of online safety at all times and to know the required procedures and to act on them. The following responsibilities demonstrate how each member of the community will contribute.

Governors

Our governors determine, support, monitor and review the school's policies. Our designated safeguarding governors have responsibility for Online Safety and will closely monitor this area and regularly meet with the Designated Safeguarding Lead(s) and other members of the Online Safety Team where appropriate to discuss developments and progress including, but not limited to:

- the effectiveness of the policy
- current issues in online safety
- reviewing (anonymised) incidents and if possible, filtering and monitoring logs

Headteacher and senior leaders:

- have a duty of care for ensuring the online safety of members of the school community and fostering a culture of safeguarding
- are responsible for ensuring that members of the online safety team, technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant
- are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role
- receive regular monitoring reports from the Online Safety Team

Designated Safeguarding Lead /Deputy Designated Safeguarding Lead (DSL/DDSL) as Online Safety Leaders supported by the E-Safety Coordinator and Online Safety Committee Leader

- will be trained in online safety issues and be aware of the potential for serious safeguarding issues to arise from: sharing of personal data, access to illegal/inappropriate materials, inappropriate online contact with adults/strangers, potential or actual incidents of grooming, online bullying.
- will take day-to-day responsibility for online safety issues, being aware of the potential for serious child protection concerns
- will promote an awareness of and commitment to online safety education/awareness both in school and out
- will ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents
- will receive reports of online safety incidents and create a log of incidents on CPOMS to inform future online safety developments
- will provide or identify sources of training and advice for staff and all other members of the school community
- will liaise with other members of the online safety team, technical, pastoral and support staff where necessary
- will meet regularly with the designated safeguarding governors to discuss current issues, review incidents and filtering and monitoring logs
- will report regularly to the headteacher and the senior leadership team
- will attend and report to, relevant governing board meetings
- will liaise with the local authority where necessary
- will liaise with subject leaders to ensure that the online safety curriculum is planned, taught, monitored and assessed effectively.

Teaching and Support Staff:

- will read, understand and implement the Online Safety policy
- will read, understand, agree and adhere to the Acceptable Use policy
- will ensure all online safety incidents are logged in line with this policy

- will maintain a professional level of conduct in personal use of technology and model safe and responsible behaviours in their own usage
- will respond appropriately to all reports and concerns about sexual violence and/or harrasment, both online and offline and maintain an attitude of 'it could happen here'.

Technical Staff (School IT Officer and LA IT Support):

- will read, understand, contribute to and help promote the Online Safety policy
- will read, understand, agree and adhere to the Acceptable Use policy
- will report any Online Safety related issues to the Online Safety Leaders
- will maintain an awareness of current online safety issues, legislation and guidance relevant to their work and pass any such information to the Online Safety Leaders
- will maintain a professional level of conduct in the personal use of technology at all times
- will support the school in providing a safe technical infrastructure to support learning and teaching
- will ensure that access to the school network is only through an authorised, restricted mechanism
- will ensure that provision exists for misuse detection and malicious attack
- will take responsibility for the security of the school ICT system and provide regular feedback to the Online Safety Leaders
- will document all technical procedures and review them for accuracy at appropriate intervals
- will restrict all administrator level accounts appropriately
- will ensure that access controls exist to protect personal and sensitive information held on school-owned devices
- will ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school
- will ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

Parents:

- will consult with the school if they have any concerns about their children's use of technology
- will help and support the school in promoting online safety
- will take responsibility for their own awareness in relation to the opportunities and risks posed by new and emerging technologies and model safe and responsible behaviours in their own usage
- will discuss online concerns with their children, show an interest in how they are using technology and encourage safe and responsible usage
- will acknowledge that they have read, understood and agree with the Acceptable Use Rules before their child starts at the school and when the child transitions to a new year group through the school diary. Parents will also be expected to update their agreement as and when the policy/statements are updated.

Visitors, volunteers 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 adhere to it and the Acceptable Use Policy.

3. Procedure for Logging Online Safety Incidents

Any online safety incidents in relation to the categories of risk set out in this policy must be reported immediately to the Online Safety Leaders face to face where necessary and logged via CPOMS.

The log must state which category of risk the incident relates to as well as all other necessary information as any other safeguarding incident (e.g. name/s of child/ren involved, date, time and location of incident).

The Online Safety Leaders will use the log of information to further investigate the incident and this may involve checking the filtering and monitoring logs, speaking with children and parents.

4. Teaching and Learning

St Mary's CE Primary School believes that the key to developing safe and responsible behaviours online, not only for children but everyone within our school community, lies in effective education.

We understand that the internet and other technologies are embedded in our children's lives both in school and out and it is our duty to prepare them to be safe online.

Children will be taught about online safety as part of the curriculum within, but not limited to Computing and Personal Development:

In Key Stage 1, children 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

In Key Stage 2, children 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, children 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
- that for most people the internet is an integral part of life and has many benefits.
- about the benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing.
- how to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private.
- why social media, some computer games and online gaming, for example, are age restricted.
- that the internet can also be a negative place where online abuse, trolling, bullying and harassment can take place, which can have a negative impact on mental health.
- how to be a discerning consumer of information online including understanding that information, including that from search engines, is ranked, selected and targeted.

- where and how to report concerns and get support with issues online. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Parents and Carers

The school will raise parents' awareness of internet safety in newsletters/letters home, and in information via the school's 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.

A partnership approach will be encouraged with parents which may include practical sessions as well as suggestions for safe internet use at home.

5. Online child on child abuse

Online child on child abuse is any form of child on child abuse with a digital element, for example, sexting, online abuse, coercion and exploitation, child on child grooming, threatening language delivered via online means, the distribution of sexualised content and harassment.

The Behaviour Policy outlines St Mary's Primary School's procedures for managing this area of online safety.

Cyber-bullying

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

The Behaviour Policy and the Anti-Bullying Policy outline St Mary's Primary School's procedures for managing these areas of online safety.

6. Acceptable Use

All pupils, parents, staff, volunteers and governors must follow the Acceptable Use, Bring your own device to work and Staff Code of Conduct policies in relation to use of the school's ICT facilities including the internet.

Further information is set out in the Acceptable Use Policy and the Staff Code of Conduct.