St. Mary's C of E Primary Academy
COLLABORATIVE LEARNING TRUST

Online Safety Policy

Introduced: January 2022

Approved: January 2022

Reviewed: September 2023

Introduction

The internet and other digital technologies are powerful resources which can enhance and transform teaching and learning when used effectively and appropriately. The internet is an essential element of 21st century life for education, business and social interaction. At St Mary's C of E Primary Academy we have a duty to provide our children with quality internet access as part of their learning experience and we are committed to ensuring that children learn how to use computers, ICT and modern technologies safely so that they:

• are able to use a range of ICT safely to support their learning in school

• are able to use ICT and modern technologies outside school in a safe manner, including using ICT as a tool for communication

• are prepared for the constant changes in the world of technology and understand how to use new and emerging technologies in a safe manner

• know what to do if they feel unsafe when it comes to using technology

Internet use will be monitored and safeguarding systems will be put in place to ensure children are safe while accessing the internet.

This policy outlines the steps we take to protect our school community from harm when using ICT and also how we proactively encourage children to develop a safe approach to using ICT whether in school or at home. The policy aims to establish clear mechanisms to identify, intervene and escalate an incident, where appropriate. This policy is written in line with 'Keeping Children Safe in Education' (2023) and 'Teaching Online Safety in Schools'.

This policy should be read alongside the following policies:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Child-on Child Abuse Policy

Our named member of staff with responsibility for Online Safety is Ms Jessica Crisp – Deputy Head teacher.

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.

Key Responsibilities

Governors

Governors are responsible for:

- ensuring that the school is implementing this policy effectively
- adhering to the acceptable use agreement when in school
- having due regard for the importance online safety in school
- **Senior Leadership Team**

The Head teacher (Mr John Davie) and the Deputy Head teacher and Designated Safeguarding Leader (Ms Jessica Crisp) are responsible for:

- ensuring this policy is implemented, communicated and monitoring compliance of the policy
- ensuring staff training on Online Safety is provided and updated annually as part of safeguarding training
- ensuring immediate action is always taken if any risks or dangers are identified i.e. reporting of inappropriate websites
- ensuring that all reported incidents of cyber bullying are investigated
- ensuring appropriate web filtering software is used to protect users from potentially damaging/offensive material
- ensuring that content on our school website is accurate and the quality of presentation is maintained
- ensuring our school website complies with the statutory guidelines

Staff Members

Staff members are responsible for:

- keeping passwords private and only using their own login details, which are stored securely
- monitor and supervising children using the internet and use of other IT resources
- adhering to the Acceptable Use Policy (September 2021)
- promoting online safety and teaching the required online safety units as part of the PSHE and computing curriculum
- engaging in online safety training
- only downloading attachments/material onto the school system if they are from a trusted source
- only using a school device when capturing images, videos or sound clips of children
- pre-checking the content of online resources when planning to use them with children

Teaching and Learning

Our aim is to deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology. We will actively teach our children about online safety at an age-appropriate level. Our PSHE scheme of work (SCARF) for each year group covers: what should and shouldn't be shared online, password control and cyber bullying among other topics. Online safety will also be embedded throughout learning whenever children are using ICT in other lessons. We will seek support from outside agencies to promote the importance of online safety for example inviting the Early Help Hub Policing Team to deliver Online Safety Workshops to KS2 children and parents/carers.

Safer Internet Day is celebrated annually across school with a range of activities to raise the profile of online safety.

We will teach the children about **content** – not all content is appropriate or reliable, **contact** – inappropriate contact may be made through digital technologies and **conduct** – inappropriate online behaviour may increase the likelihood of harm to themselves and others.

Monitoring Safe and Secure Systems

At St. Mary's C of E Primary Academy Internet access is regulated by XXX (to be updated in October 2023). This protects the school from attacks from the internet and blocks access to certain categories of website. It provides a tried and tested, secure and highly successful filtering system ensuring confidence in internet access at our school. Termly checks are carried out by the designated safeguarding team to check that the filtering system is effective.

We take all reasonable precautions to ensure that our users only access appropriate material however, no firewall is ever 100% effective. Children will be taught the necessary skills to manage risks themselves on an age appropriate level. If staff or pupils discover an inappropriate website it must be reported to the Designated Safeguarding Leader (DSL) – Ms Jessica Crisp.

The PREVENT Duty: Under the PREVENT Duty we are legally required to take steps to prevent children from being drawn into terrorism. We take this duty seriously and carry out the four main actions responsibly, namely: risk assessment, working in partnership, staff training and IT policies. We recognise that we play a vital role in keeping children safe from harm, including from the risks of extremism and radicalisation, and in promoting the welfare of children in our care. The filtering systems in place are compliant with the PREVENT Duty and any internet use that is in violation of this duty is automatically reported to the DSL. All staff have up to date PREVENT duty training and this will be updated as required.

The School Website

Our school website will be used to celebrate children's work, promote the school and share information with parents and carers. Clear ground rules are established to ensure that the website reflects our ethos and that the information is accurate and well presented. As the school's website can be accessed by anyone on the Internet, the security of staff and children is carefully considered. Publishing children's names alongside their photograph is inappropriate and only first names will be used. Parents / Carers will be asked annually for consent regarding the use of their child's photo on our website and on social media.

Social Media

Parents and carers will be advised that the use of social network spaces outside school is inappropriate for primary aged children and this will be reiterated to children in school. We recognise that as a school we have a duty to help children stay safe when they are accessing the internet and using apps at home and we will cover such issues within the curriculum.

Staff must not make any reference on social media to children, parents/carers, school staff or any issues/situations related to the school.

Communications

School email accounts and Arbor are used for communications between school and home. The use of personal email addresses, text messaging or social media is not permitted to communicate to parents/carers or children. Staff must ensure they are professional in tone and content and they are not expected to reply to e mails out of school hours.

Remote Learning

Remote learning must follow guidelines issued in the Remote Learning Policy (2020). These include actions such as: attendance, supervision, appropriate dress and guidance around appropriate communication. Remote learning must also maintain the same child protection and safeguarding protocols that apply in the normal school environment including the staff and parent/carer/child acceptable use policies. The Senior Leadership Team are responsible for monitoring the security of remote learning systems, including data protection and safeguarding considerations with I.T support.

Acceptable Use

We have an Acceptable Use Policy in place and staff are asked to sign to say they have received, read and understood the policy. Any new staff starting during the school year will be issued with this policy as part of their induction. Visitors to school will be issued with a Visitor Guide.

The use of mobiles is discouraged throughout the school. However, mobile phones may be carried by staff in the case of an emergency. The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying.

Staff using work devices outside of school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in the Acceptable Use Policy. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

a

Responding to Incidents of Online Safety

All members of the school community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively. Support will be actively sought from other agencies as needed (i.e. MASH, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, Internet Watch Foundation) in dealing with online safety issues. Parents/carers will be specifically informed of online safety incidents involving their child. The Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

Where a child misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour and Relationships Policy and Acceptable Use Policy. 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 code of conduct. The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

All Online Safety incidents should be recorded on CPOMs under Cause for Concern: Online Safety. The DSL will monitor all incidents on CPOMs half-termly. incident.

Examples of illegal offences are:

- accessing child sexual abuse images
- accessing non-photographic child sexual abuse images
- accessing criminally obscene adult content
- incitement to racial hatred inappropriate

Educating Parents / Carers about Online Safety

"Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it." (Byron Report, 2008)

At St. Mary's C of E Primary Academy we will raise parents/carers awareness of online safety in letters home and in information on our website. This policy is available on our school website for parents/carers. If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head teacher (Mr John Davie) and/or the DSL (Ms Jessica Crisp).