Online Safety Policy

Governor Review Date	Autumn 2024
Review Frequency	Annual
Date for Next Review	Autumn 2025
Head Teacher Approval	Autumn 2024
Governor Approval	Autumn 2024

The Online Safety Policy has been written by the school, incorporating points from the Department for Education's (DfE) statutory guidance 'Keeping Children Safe in Education', its non-statutory guidance 'Teaching Online Safety in Schools' and a number of other carefully selected sources. The policy has been agreed by the leadership team and approved by the Governing Body. It will be reviewed regularly and updated at least annually. Changes will be made immediately if technological or other developments require it.

Online Safety Risks

The Department for Education published an updated version of 'Keeping children safe in education' in 2024.

It states the following:

1. All staff should be aware of indicators of abuse and neglect (see below), understanding that children can be at risk of harm inside and outside of the school, inside and outside of home and online. Exercising professional curiosity and knowing what to look for is vital for the early identification of abuse and neglect so that staff are able to identify cases of children who may be in need of help or protection. All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

2. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

3. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

3.1 content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism;

3.2 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'.

3.3 conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, 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; and

3.4 commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. The importance of staff understanding the role that children can plan in abusing other children is highlighted in the document: Child on Child Abuse Policy (addendum to the Safeguarding Policy).

4. All staff should be aware that children can abuse other children (often referred to as child-on-child abuse), and that it can happen both inside and outside of school and online. All staff should be clear as to the school's policy and procedures with regard to child-on-child abuse and the important role they have to play in preventing it and responding where they believe a child may be at risk from it. More detail on this matter is included in the school's Safeguarding Policies. The following sections of this policy address the above risks and the systems in place to reduce the risk both within school and for our children in their home lives.

Filters and monitoring

Statutory guidance from the 2024 update of KCSIE dictates the following:

5. Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs verses safeguarding risks. An addition to this year's KCSIE update includes specific expectations around filtering and monitoring in schools and directs education settings to the updated document 'Meeting digital and technology standards in schools and colleges':

6. To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

• identify and assign roles and responsibilities to manage filtering and monitoring systems.

• review filtering and monitoring provision at least annually.

• block harmful and inappropriate content without unreasonably impacting teaching and learning.

• have effective monitoring strategies in place that meet their safeguarding needs.

Governing bodies and proprietors should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

Additional guidance on filtering and monitoring can be found at: UK Safer Internet Centre: “appropriate” filtering and monitoring. https://www.saferinternet.org.uk/advicecentre/teachers-and-school staff/appropriate-filtering and-monitoring. Southwest Grid for Learning (swgfl.org.uk) have created a tool to check whether a school or college’s filtering provider is signed up to relevant lists (CSA content, Sexual Content, Terrorist content, Your Internet Connection Blocks Child Abuse & Terrorist Content)

7. Online safety and the school or college’s approach to it should be reflected in the child protection policy. Considering the 4Cs (above) will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and 36 smart technologies. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and nonconsensual (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.