

KCSIE – September 2023 update

What school and college staff need to know

14. All staff should receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – see para 141 for further information) at induction. The training should be regularly updated. In addition, **all** staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.

Staff training

124. Governing bodies and proprietors should ensure that **all** staff undergo safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – see para 141 for further information) at induction. The training should be regularly updated. Induction and training should be in line with any advice from the safeguarding partners.

Online safety policy

138. Online safety and the school or college's approach to it should be reflected in the child protection policy which, amongst other things, should include appropriate filtering and monitoring on school devices and school networks. 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 smart technology, which will also 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 non-consensually (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.

Filtering and monitoring

141. 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 filtering 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 number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

142. The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty.

Children potentially at greater risk of harm

170. Whilst **all** children should be protected, it is important that governing bodies and proprietors recognise (and reflect in their policies and procedures) that some groups of children, are potentially at greater risk of harm than others (both online and offline).