Online Safety within 'Keeping Children Safe in Education' 2023

The internet and technology are every day and essential tool for learning and socialising. The online safety agenda continues to evolve and increase, and it continues to be crucial that schools and colleges recognise online safety as a key safeguarding consideration and part of their statutory safeguarding responsibilities. DSLs, governing bodies and proprietors should understand and be able to evidence the recognition of online safety within their statutory safeguarding responsibilities and implement approaches which will safeguard their community online.

Keeping Children Safe in Education 2023

On the 6th June 2023 the Department for Education (DfE) published the updated 'Keeping children safe in education' (KCSIE) guidance ready for implementation from the 1st September 2023. Schools and Colleges must comply with KCSIE 2022 until that date.

'Keeping children safe in education' (KCSIE) is statutory guidance from the Department for Education. Schools and colleges in England must have regard to it when carrying out their duties to safeguard and promote the welfare of children. For the purposes of the guidance, 'children' includes everyone under the age of 18.

The DfE use the terms "must" and "should" throughout the guidance; "must" is used when the person in question is legally required to do something and "should" when the advice set out should be followed unless there is good reason not to.

The KCSIE guidance should be read alongside:

- statutory guidance Working Together to Safeguard Children, and
- departmental advice What to do if you are Worried a Child is Being Abused - Advice for Practitioners

This document only focuses on elements of KCSIE 2023 relevant to **online safety**. Designated Safeguarding Leads (DSLs) and leaders should read KCSIE 2023 in its entirety when considering their wider safeguarding practice requirements from 1st September 2023.

Summary of online safety changes/additions within KCSIE 2023

- Content has been added regarding expectations about content to be covered in relation to staff online safety training providing an 'understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring'.
- Clarification added to emphasise the designated safeguarding leads responsibility for online safety, including understanding the filtering and monitoring systems and processes in place.
- An expectation that the school/college child protection policy should address appropriate filtering and monitoring on school devices and school networks.
- Additional content to reflect that filtering and monitoring decisions should consider 'those who are potentially at greater risk of harm and how often they access the IT system.'
- New links to direct schools to consider how they are meeting the DfE 'Filtering and monitoring standards for schools and colleges' and 'Cyber security standards for schools and colleges'

Online Safety within 'Keeping Children Safe in Education' 2023

- Clarification in part three that schools and colleges should inform shortlisted candidates that online searches may be done as part of due diligence checks.

Summary of online safety requirements within KCSIE

- The DSL has overall responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place; they can be supported by appropriately trained deputies and should liaise with other staff as appropriate, but this responsibility cannot be delegated.
- DSLs should evidence that they have accessed appropriate training and/or support to ensure they understand the unique risks associated with online safety, can recognise the additional risks learners with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe online.
- All staff (including governors and trustees) should receive appropriate safeguarding and child protection training, including online safety at induction. This should amongst other things, include an understanding of the expectations, applicable roles, and responsibilities in relation to filtering and monitoring.
- Online safety should also be addressed as part of regular (at least annual) child protection training and staff should receive updates, as appropriate.
- Children should be taught about online safety, including as part of statutory Relationships and Sex Education (RSE), however schools and colleges should recognise that a one size fits all approach may not be appropriate, and a more personalised or contextualised approach for more vulnerable children e.g., victims of abuse and SEND, may be needed.
- Schools/colleges should be doing all that they reasonably can to limit children's exposure to risks from the school's or college's IT system and should ensure they have appropriate filtering and monitoring systems in place and regularly review their effectiveness. The leadership team and relevant staff should have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns identified. When making filtering and monitoring decisions, schools/colleges should consider 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.
- Schools/colleges should recognise that child-on-child abuse, including sexual violence and sexual harassment can occur online. School/colleges have an essential role to play in both preventing online child-on-child abuse and responding to any concerns when they occur, even if they take place offsite and should have appropriate systems in place to support and evidence this.
- Schools/colleges should ensure their child protection policy and wider safeguarding policies specifically address online safety, especially with regards to appropriate filtering and monitoring on school devices and school networks, child-on-child abuse, relationships on social media and the use of mobile and smart technology.
- Schools/colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the specific risks their children face.

What this means for DSLs and leaders

- Online safety should be viewed as part of your school/college statutory safeguarding responsibilities and will require a whole school/college approach.

Online Safety within 'Keeping Children Safe in Education' 2023

- Ensure your DSL is recognised as having overall responsibility for online safety, and that they access appropriate training and support to enable them to keep up to date.
- Ensure your safeguarding policies (including your child protection policy), education approaches and staff training address the breadth of online safety issues as identified in KCSIE; content, contact, conduct and commerce.
- Update your child protection (and/or online safety policies if you have a standalone document) and behaviour policies to address appropriate filtering and monitoring on school devices and school networks, online child-on-child abuse, and the use of mobile and smart technology on your premises.
- Ensure your staff behaviour policy specifically covers acceptable use of technologies, including the use of mobile devices, staff/pupil relationships and communications, including the use of social media.
- Work with curriculum leads (especially RSE leads) to ensure there is a range of opportunities within the curriculum for children to be taught about online safety in a way that is appropriate to their age and needs.
- Ensure all staff, including governors and trustees are provided with appropriate and up-to-date online safety information and training at induction, and as part of regular child protection training and updates
- Staff training should include an 'understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring'.
- All staff should be made aware of the policies and procedures to follow with regards to responding to online safety concerns, including online child-on-child abuse issues.
- DSLs should access the UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' and the DfE 'Harmful online challenges and online hoaxes' guidance to ensure they are familiar with its content and when it should be followed.
- Schools/colleges should ensure appropriate filtering and monitoring approaches are in place which are suitable for the local context and use of technology. The leadership team and relevant staff should have an awareness and understanding of the appropriate filtering and monitoring provisions in place, manage them effectively and know how to escalate concerns when identified.
- DSLs and school/colleges leaders should access the DfE 'Filtering and monitoring standards for schools and colleges' and 'Cyber security standards for schools and colleges' and consider how the school/college is meeting the requirements, and if any further action is required.
- The school/college recruitment process should be transparent and ensure that shortlisted candidates are aware that online searches may be done as part of due diligence checks.
- There should be regular and appropriate parental engagement in online safety, and specific concerns should be responded to in line with child protection policies.
- DSLs should ensure online safety approaches are regularly reviewed and supported by an annual risk assessment that considers and reflects the specific risks their children face.

Online Safety Support Available from the Education Safeguarding Service

Specific guidance and information regarding online safety can be found on the Education Safeguarding Service area of our website – this includes links to national guidance and resources and template policies for schools and settings to adapt.

Online Safety within 'Keeping Children Safe in Education' 2023

Our Safeguarding Support Package for Schools is available to schools and colleges in Kent and beyond and includes several online safety resources for DSLs and school leaders, including template online safety staff training resources, a specific online safety policy and briefings for DSLs.

The Education Safeguarding Service provide a number of training courses, services and standalone products (including an online safety policy toolkit and guidance on official use of social media) which can help support schools and colleges update their online safety practice.

Kent education settings can contact the online safety team within the Education Safeguarding Service to discuss available support and training to enable them to fulfil their statutory safeguarding requirements regarding online safety.

How to read/use this document

- This font indicates a direct quote from the KCSIE 2023 guidance.
- This font indicates where KCSIE identifies online safety specific content.
- This font is used to raise and explore practice considerations and highlight best practice recommendations and useful links.
- This font indicates an action point for DSLs and school/college leaders to consider in readiness for September 2023.

Disclaimer

The document has been written by Rebecca Avery, Training and Development Manager and Online Safety Lead within the Education Safeguarding Service at Kent County Council in June 2023.

Kent County Council will make every effort to ensure that the information in this document is accurate and up to date. If errors are brought to our attention, we will correct them as soon as practicable.

Online Safety within 'Keeping Children Safe in Education' 2023

Keeping Children Safe in Education 2023

Part One: Safeguarding information for all staff

What school and college staff need to know

13. **All** staff should be aware of systems within their school or college which support safeguarding, and these should be explained to them as part of staff induction. This should include the:

- child protection policy (which should amongst other things also include the policy and procedures to deal with child-on-child abuse)
- behaviour policy (which should include measures to prevent bullying, including cyberbullying, prejudice-based and discriminatory bullying)
- staff behaviour policy (sometimes called a code of conduct) should amongst other things, include low-level concerns, allegations against staff and whistleblowing…
- …role of the designated safeguarding lead (including the identity of the designated safeguarding lead and any deputies).

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.

18. **All** staff should be able to reassure victims that they are being taken seriously and that they will be supported and kept safe. A victim should never be given the impression that they are creating a problem by reporting any form of abuse and/or neglect. Nor should a victim ever be made to feel ashamed for making a report.

19. **All staff** should be aware that children may not feel ready or know how to tell someone that they are being abused, exploited, or neglected, and/or they may not recognise their experiences as harmful. For example, children may feel embarrassed, humiliated, or being threatened. This could be due to their vulnerability, disability and/or sexual orientation or language barriers. This should not prevent staff from having a professional curiosity and speaking to the DSL if they have concerns about a child. It is also important that staff determine how best to build trusted relationships with children and young people which facilitate communication.

What school and college staff should look out for: Abuse and neglect

24. 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.

25. In all cases, if staff are unsure, they should always speak to the designated safeguarding lead (or deputy).

Practice Implications

- All staff should receive information and training which addresses online safety at induction, and as part of accessing regularly updated safeguarding and child protection training and information.
- **Para 14. New text added to raise awareness of the existing expectation for relevant staff to understand filtering and monitoring**; all staff should understand the expectations, applicable roles, and responsibilities in relation to filtering and monitoring in place on school/college devices and networks.
- Staff should be aware that children may not feel ready or know how to tell someone they are being abused; this is especially likely to be the case where abuse takes place online.
- Online safety concerns should be reported to the DSL or a deputy.

Action points

- Does your staff training (at induction and as part of annual updates) provide staff with an understanding on the expectations, applicable roles, and responsibilities in relation to filtering and monitoring in place on school/college devices and networks?
- Does your child protection policy make is clear that all online safety concerns should be reported to the DSL?

Indicators of abuse and neglect

26. Abuse: a form of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm or by failing to act to prevent harm…. Children may be abused in a family or in an institutional or community setting by those known to them or, more rarely, by others**.** Abuse can take place wholly online, or technology may be used to facilitate offline abuse. Children may be abused by an adult or adults or by another child or children.

28. **Emotional abuse**: the persistent emotional maltreatment of a child such as to cause severe and adverse effects on the child's emotional development. It may involve …serious bullying (including cyberbullying) causing children frequently to feel frightened or in danger, or the exploitation or corruption of children. Some level of emotional abuse is involved in all types of maltreatment of a child, although it may occur alone.

Practice Implications

- This specifically identifies that cyberbullying can become emotional abuse.
- School/college anti-bullying policies should be up-to-date and include approaches to dealing with all forms of bullying, including cyberbullying.

- The DfE preventing and tackling bullying guidance (which includes cyberbullying) can be found here.
- Childnet provide targeted information regarding cyberbullying: Childnet: Cyberbullying guidance
- Schools who are members of our Education Safeguarding Support Package have access to an anti-bullying policy template. The anti-bullying policy template, along with additional online safety guidance and our online safety policy template are available to purchase standalone.

Action points

- Does your anti-bullying policy specifically address the measures you have in place to both prevent and respond to cyberbullying?
- Does your anti-bullying and/or child protection policy outline the procedures to follow if cyberbullying concerns are reported?

29. **Sexual abuse:** involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing, and touching outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. Sexual abuse can take place online, and technology can be used to facilitate offline abuse. Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children. The sexual abuse of children by other children is a specific safeguarding issue in education and **all** staff should be aware of it and of their school or college's policy and procedures for dealing with it.

Practice Implications

- This specifically identifies that sexual abuse can occur via the internet and can involve a range of online behaviours.

Action points

- Are all staff aware of online sexual abuse, including the possible risk of online sexual abuse of children by other children.

Safeguarding issues

31. **All** staff should have an awareness of safeguarding issues that can put children at risk of harm. Behaviours linked to issues such … consensual and non-consensual sharing of nude and semi-nude images and/or videos can be signs that children are at risk.

Practice Implications

- This specifically identifies that all staff should recognise consensual and non-consensual sharing of nude and semi-nude images and/or videos as a safeguarding issue and know how to respond to concerns.
- The footnote recognises that consensual image sharing, especially between older children of the same age, may require a different response and might not be abusive, however, children still need to know it is illegal, whilst non-consensual is illegal and abusive. The footnote also signposts to the more detailed advice about sharing of nudes and semi-nude images and videos by UK Council for Internet Safety (UKCIS).

Child-on-child abuse

32. **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 or college and online. **All** staff should be clear as to the school's or college'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.

Practice Implications

- All members of staff should recognise the range of online child-on-child abuse safeguarding issues and understand how they should respond to and report concerns.

33. **All** staff should understand that even if there are no reports in their schools or colleges it does not mean it is not happening, it may be the case that it is just not being reported. As such it is important if staff have **any** concerns regarding child-on-child abuse they should speak to their designated safeguarding lead (or deputy).

Practice Implications

- This is especially likely to be the case where there are online child-on-child abuse concerns. For example, learners frequently report they are unlikely to report concerning online behaviours if they are using what adults consider to be 'inappropriate' social media platforms or gaming sites.

34. It is essential that **all** staff understand the importance of challenging inappropriate behaviours between children, many of which are listed below, that are abusive in nature. Downplaying certain behaviours, for example dismissing sexual harassment as "just banter", "just having a laugh", "part of growing up" or "boys being boys" can lead to a culture of unacceptable behaviours, an unsafe environment for children and in worst case scenarios a culture that normalises abuse leading to children accepting it as normal and not coming forward to report it.

Practice Implications

- This should include staff understanding the importance of challenging inappropriate behaviours which take place online.

35. Child-on-child abuse is most likely to include, but may not be limited to:

- bullying (including cyberbullying, prejudice-based and discriminatory bullying)
- abuse in intimate personal relationships between children (sometimes known as 'teenage relationship abuse')
- physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm (this may include an online element which facilitates, threatens and/or encourages physical abuse)
- sexual violence, such as rape, assault by penetration and sexual assault; (this may include an online element which facilitates, threatens and/or encourages sexual violence)
- sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse
- causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
- consensual and non-consensual sharing of nude and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery)
- upskirting which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress, or alarm, and
- initiation/hazing type violence and rituals (this could include activities involving harassment, abuse or humiliation used as a way of initiating a person into a group and may also include an online element).

Practice Implications

- It should be clearly recognised that technology can play a key role within child-on-child abuse concerns. Schools and colleges should therefore ensure they reflect this within appropriate policies, procedures and approaches and ensure all staff receive appropriate information and training.

Action points

- Does your child protection policy clearly recognise the range of online child-on-child abuse issues?
- Does your policy detail how to report concerns relating to online child-on-child abuse?
- Do you provide training to all members of staff regarding online child-on-child abuse?

Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)

36. Both CSE and CCE are forms of abuse that occur where an individual or group takes advantage of an imbalance in power to coerce, manipulate or deceive a child into taking part in sexual or criminal activity, in exchange for something the victim needs or wants, and/or for the financial advantage or increased status of the perpetrator or facilitator and/or through violence or the threat of violence. CSE and CCE can affect children, both male and female and can include children who have been moved (commonly referred to as trafficking) for the purpose of exploitation

Online Safety within 'Keeping Children Safe in Education' 2023

Child Criminal Exploitation (CCE)

Practice Implications

- Although not specifically mentioned in part one, it is important to recognise that CCE can be facilitated by technology; for example, gangs may target young people via social media, or provide devices in exchange for or to support criminal activity. This is addressed in Annex B.

Child Sexual Exploitation (CSE)

40. CSE is a form of child sexual abuse. Sexual abuse may involve physical contact, including assault by penetration (for example, rape or oral sex) or nonpenetrative acts such as masturbation, kissing, rubbing, and touching outside clothing. It may include noncontact activities, such as involving children in the production of sexual images, forcing children to look at sexual images or watch sexual activities, encouraging children to behave in sexually inappropriate ways or grooming a child in preparation for abuse including via the internet.

37. CSE can occur over time or be a one-off occurrence and may happen without the child's immediate knowledge for example through others sharing videos or images of them on social media.

Practice Implications

- This specifically identifies that CSE can take place online or be facilitated by technology. Further information about CSE including definitions and indicators is included in Annex B

Domestic Abuse

43. Domestic abuse can encompass a wide range of behaviours and may be a single incident or a pattern of incidents. That abuse can be, but is not limited to, psychological, physical, sexual, financial or emotional. Children can be victims of domestic abuse. They may see, hear, or experience the effects of abuse at home and/or suffer domestic abuse in their own intimate relationships (teenage relationship abuse). All of which can have a detrimental and long-term impact on their health, well-being, development, and ability to learn.

Practice Implications

- Whilst online safety is not specifically mentioned in this paragraph, it is important to be aware that technology can be used as a tool to facilitate domestic abuse, for example coercive control, cyberstalking and sharing or threatening to share intimate images.

Online Safety within 'Keeping Children Safe in Education' 2023

Part two: The management of safeguarding

Legislation and the law

78. Governing bodies and proprietors have a strategic leadership responsibility for their school's or college's safeguarding arrangements and **must** ensure that they comply with their duties under legislation. They **must** have regard to this guidance, ensuring policies, procedures and training in their schools or colleges are effective and comply with the law at all times. Headteachers and principals should ensure that the policies and procedures, adopted by their governing bodies and proprietors (particularly those concerning referrals of cases of suspected abuse and neglect), are understood, and followed by all staff.

Practice Implications

- This applies to duties relating to online safety practice.

81. Governing bodies and proprietors should ensure that **all** governors and trustees receive appropriate safeguarding and child protection (including online) training at induction. This training should equip them with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures in place in schools and colleges are effective and support the delivery of a robust whole school approach to safeguarding. Their training should be regularly updated.

Practice Implications

- All governors and trustees should receive appropriate online safety information as part of their safeguarding and child protection training which they receive as part of their induction and this training should be regularly updated. We would recommend this training forms part of your existing approaches to safeguarding and child protection training for all staff, for example, as part of your induction process and at least annual child protection updates. The guidance does not go into depth regarding how this can/should be achieved, so schools and colleges may wish to consider different approaches; for example, accessing appropriate externally provided training, or internal training, for example training provided by the DSL.
- Training for governors and trustees will not be the same as training for staff; whilst it can be helpful for governors to attend the school/college child protection training for quality assurance purposes, their training should specifically focus on the role of the governor to enable them to understand their strategic role and responsibilities regarding online safety, and should ensure they are confident to ask appropriate questions to assure themselves that online safety policies and procedures are in place in their setting, and that they are effective and support the delivery of a robust whole school approach to online safety.

Action points

- Do your governors and trustees access online safety training as part of the induction process?
- How will you ensure this training is updated?
- Does the training specifically address the strategic roles and responsibilities for governors and trustees in relation to online safety?

Online Safety within 'Keeping Children Safe in Education' 2023

Whole school and college approach to safeguarding

95. Governing bodies and proprietors should ensure they facilitate a whole school or college approach to safeguarding. This means involving everyone in the school or college, and ensuring that safeguarding, and child protection are at the forefront and underpin all relevant aspects of process and policy development. Ultimately, all systems, processes and policies should operate with the **best interests** of the child at their heart.

96. Where there is a safeguarding concern, governing bodies, proprietors and school or college leaders should ensure the child's wishes and feelings are taken into account when determining what action to take and what services to provide.

97. The school's or college's safeguarding policies and procedures (some of which are listed below) should be transparent, clear, and easy to understand for staff, pupils, students, parents, and carers. Systems should be in place, and they should be well promoted, easily understood and easily accessible for children to confidently report, any form of abuse or neglect, knowing their concerns will be treated seriously, and knowing they can safely express their views and give feedback.

Practice Implications

- Online safety should be integrated into the whole school/college approach to safeguarding.

Safeguarding policies and procedures

98. Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare.

99. These policies should include individual schools and colleges having:

- an **effective child protection policy** which:
  - reflects the whole school/college approach to child-on-child abuse
  - includes policies as reflected elsewhere in Part two of this guidance, such as online safety…,
  - is reviewed annually (as a minimum) and updated if needed, so that it is kept up to date with safeguarding issues as they emerge and evolve, including lessons learnt; and
  - is available publicly either via the school or college website or by other means

Practice Implications

- Individual schools/colleges should have a specific and robust child protection policy which is updated at least annually and is publicly available.
- If possible, staff should be involved in the development and construction of policies to promote ownership and understanding. This could involve including staff in development via discussions at staff meetings or reviewing policies with staff working groups.

- a **behaviour policy** which includes measures to prevent bullying (including cyberbullying, prejudice-based and discriminatory bullying)

Online Safety within 'Keeping Children Safe in Education' 2023

- a **staff behaviour policy** (sometimes called the code of conduct) which should, amongst other things, include… acceptable use of technologies (including the use of mobile devices), staff/pupil relationships and communications including the use of social media.

Practice Implications

- The staff behaviour policy should explicitly cover expectations regarding professional conduct online.
- All staff should read and understand the relevant policies and procedures and they should be reviewed at least annually.
- The Education Safeguarding Service provide a template Acceptable Use Policy (AUP) which can help schools and colleges develop their staff behaviour policy.

100. …. These policies and procedures, along with Part one (or Annex A if appropriate) of this guidance and information regarding the role and identity of the designated safeguarding lead (and deputies), should be provided to all staff on induction.

Practice Implications

- All members of staff should be provided with appropriate information (including online safety, child-on-child abuse, acceptable use of technologies, staff/pupil relationships and the use of social media) as part of induction.
- Paragraph 100 states that governing bodies and proprietors should take a proportionate risk-based approach to the level of information that is provided to temporary staff, volunteers, and contractors, however when it comes to the safer use of technology, this may be necessary depending on the context. For example, providing guidance to contractors on how mobile devices can or cannot be used on your premises, or guidance to parents' volunteers regarding confidentiality and the use of social media.

Action points:

- Is online safety appropriately addressed in your child protection policy, or appropriately cross referenced if you have a standalone online safety policy?
    - Is your child protection policy up to date (reviewed at least annually) and available publicly?
- Does your behaviour policy include measures to prevent and tackle cyberbullying?
- Does your staff behaviour policy/code of conduct cover the acceptable use of technology for staff, online staff/pupil relationships and communication via social media?
    - Is it up to date?
    - How do you ensure that this information is communicated with and understood by all members of staff?
    - How do you evidence this?
- Are these policies shared with all staff on induction?
- How do you share policy changes or updates with staff?
    - What information do you share with temporary staff, volunteers and contractors?

Online Safety within 'Keeping Children Safe in Education' 2023

The designated safeguarding lead

103. Governing bodies and proprietors should ensure an appropriate **senior member** of staff, from the school or college **leadership team**, is appointed to the role of designated safeguarding lead. It is not appropriate for the proprietor to be the designated safeguarding lead. The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role-holder's job description.

104. Governing bodies and proprietors should ensure the designated safeguarding lead has the appropriate status and authority within the school or college to carry out the duties of the post. The role carries a significant level of responsibility and the postholder should be given the additional time, funding, training, resources, and support needed to carry out the role effectively.

105. It is for individual schools and colleges to decide whether they choose to have one or more deputy designated safeguarding leads. Any deputy (or deputies) should be trained to the same standard as the designated safeguarding lead.

106. See Annex C, which describes the broad areas of responsibility and activities related to the role.

Practice Implications

- **Updated:** The overall responsibility for online safety is explicitly held by the Designated Safeguarding Lead (DSL) and this should not be delegated. Paragraph 103 has been updated for 2023 to clarify that DSLs have a responsibility to understand the filtering and monitoring systems and processes in place within the school/setting.
- Staff with appropriate skills, interest and expertise regarding online safety (such as computing leads or technical staff) can support the DSL, for example when developing curriculum approaches or making technical decisions, however overall responsibility cannot be delegated.
- Individual schools and colleges may decide to have one or more deputy designated safeguarding leads to support with online safety, however they should be trained to the same standard as the DSL.

Action points:

- Is your DSL clearly recognised as having overall responsibility for online safety?
    - Is this made clear to all members of staff?
- Have you identified other members of staff who have skills, expertise or interests who may be able to support the DSL? If appropriate, have they had specific training to enable them to act as a deputy DSL?

Online Safety within 'Keeping Children Safe in Education' 2023

Information sharing

Practice Implications

- Paragraphs 115 to 123 explore responsibilities with regarding to information sharing, including the transfer of records.
- Schools/colleges have a responsibility to ensure electronic systems as well as paper recording systems are kept in line with data protection legislation.
- DSLs and SLT should be aware of the possible implications and ensure appropriate precautions and action are taken to ensure information held electronically is kept, stored and transferred in accordance with data protection legislation.
- Paragraph 122 should also include the DSL sharing information with the new school/college in advance of a child leaving if there have been any online safety concerns.

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.

125. In addition, all staff should receive regular safeguarding and child protection updates, including online safety (for example, via email, e-bulletins, staff meetings) as required, and at least annually, to provide them with relevant skills and knowledge to safeguard children effectively.

126. Governing bodies and proprietors should recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns on a daily basis. Opportunity should therefore be provided for staff to contribute to and shape safeguarding arrangements and the child protection policy

127. Governing bodies and proprietors should ensure that, as part of the requirement for staff to undergo regular updated safeguarding training, including online safety and the requirement to ensure children are taught about safeguarding, including online safety, that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.

128. Whilst considering the above training requirements, governing bodies and proprietors should have regard to the Teachers' Standards which set out the expectation that all teachers manage behaviour effectively to ensure a good and safe educational environment and requires teachers to have a clear understanding of the needs of all pupils.

Practice Implications

- Child protection training should explicitly cover online safety as part of all staff members induction.
    - Schools and colleges should ensure online safety is specifically covered within annual safeguarding updates provided to staff.
- **Para 124. New text added** to make clear staff training should include understanding roles and responsibilities in relation to filtering and monitoring; all staff should understand the expectations,

applicable roles and responsibilities in relation to filtering and monitoring in place on school/college devices and networks.

- Settings should consider how this training will be implemented; for example, if it will be integrated within existing safeguarding and child protection training or provided as separate and specific online safety inputs.
    - Schools and colleges may decide to integrate online safety within current child protection training or provide separate sessions. Local good practice examples for staff training identified by the Education safeguarding Service include covering safeguarding (including online safety) as a standing item at staff meetings and providing specific online safety training as part of an annual training calendar of staff training events.
    - Where schools are using external providers to facilitate/deliver staff training, it is important to consider if this training is able to provide staff with information required to understand their roles and responsibilities in relation to the filtering and monitoring systems in place within your school/college. It is unlikely that a generic eLearning course for example can provide details on your specific systems and expectations, therefore, additional staff training is likely to be required to fulfil this requirement.
- Online safety training should be accessed by ALL members of staff, not just teaching staff. A child could disclose an online safety concern to any adult; therefore, all members of staff should be aware of how to recognise, respond to, record, and refer online safety concerns.

Action points:

- Is online safety covered explicitly within your induction process for new staff?
- How does your school/college provide appropriate, up-to-date, and relevant whole staff online safety training on an ongoing basis?
- Does your straining provide all staff with an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring approaches in place within your school/setting?
- Does your staff training cover professional online practice issues (such as use of social media, classroom management etc.) as well as safeguarding children and young people?
- How do you share regular online safety information and updates with staff outside of formal training, for example, via email, e-bulletins, and staff meetings?
- How do you evidence all of this is in place?

Opportunities to teach safeguarding

129. Governing bodies and proprietors should ensure that children are taught about how to keep themselves and others safe, including online. It should be recognised that effective education will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs or disabilities.

130. In schools, relevant topics will be included within Relationships Education (for all primary pupils), and Relationships and Sex Education (for all secondary pupils) and Health Education (for all primary and secondary pupils). In teaching these subjects schools must have regard to the statutory guidance, which can be found here. Colleges may cover relevant issues through tutorials.

Online Safety within 'Keeping Children Safe in Education' 2023

131. Schools and colleges play a crucial role in preventative education. Preventative education is most effective in the context of a whole-school or college approach that prepares pupils and students for life in modern Britain and creates a culture of zero tolerance for sexism, misogyny/misandry, homophobia, biphobic and sexual violence/harassment. The school/college will have a clear set of values and standards, upheld and demonstrated throughout all aspects of school/college life. These will be underpinned by the school/college's behaviour policy and pastoral support system, as well as by a planned programme of evidence based RSHE delivered in regularly timetabled lessons and reinforced throughout the whole curriculum. Such a programme should be fully inclusive and developed to be age and stage of development appropriate (especially when considering the needs of children with SEND and other vulnerabilities). This program will tackle at an age-appropriate stages issues such as:

- healthy and respectful relationships
- boundaries and consent
- stereotyping, prejudice and equality
- body confidence and self-esteem
- how to recognise an abusive relationship, including coercive and controlling behaviour
- the concepts of, and laws relating to- sexual consent, sexual exploitation, abuse, grooming, coercion, harassment, rape, domestic abuse, so called honour-based violence such as forced marriage and Female Genital Mutilation (FGM), and how to access support, and
- what constitutes sexual harassment and sexual violence and why these are always unacceptable.

Practice Implications

- Paragraphs 132 and 133 refer to resources that support effective teaching of safeguarding topics, including online safety. Paragraph 133 includes the DfE 'Harmful online challenges and online hoaxes' guidance which includes advice on preparing for any online challenges and hoaxes, sharing information with parents and carers and where to get help and support.
- The bullet points in paragraph 130 will all need to address online safety messages as part of providing preventative education and to be effective in preparing learners for life in modern Britain and creating a zero-tolerance culture.
- Governing bodies and proprietors should ensure that online safety is specifically covered within their curriculum.
    - Online safety education should be flexible, relevant and engage learners' interests, and encourage them to develop resilience to online risks.
    - Education approaches should take into account local content and any specific vulnerabilities for learners, for example, children with SEND or mental health needs, children in care or children who have experienced abuse.
- The responsibility for teaching children about online safety is not the sole responsibility of the computing curriculum; only teaching online safety to children as part of ICT or computing could lead to a focus on technical issues and may not fully explore or address underlying behaviours or safeguarding risks. Online safety should be taught as part of school and colleges RSE approaches and be woven throughout the curriculum for all age groups. Paragraph 133 and 134 signposts to specific resources which could support online safety education, including:
    - The DfE advice, 'teaching online safety in schools' and UKCIS 'Education for a Connected World' Framework will help schools and colleges explore online safety education approaches in more depth.

    - The SWGfL have produced Project Evolve which aims to provide education resources in line with the strands identified within 'Education for a connected world' framework.
- Schools and colleges should ensure they use a range of relevant resources and be mindful that online safety educate content can date quickly due to the rapid pace of change within technology.
    - Good practice would be to gain learner input into the online safety curriculum; this could involve use of student/pupil councils or use of peer education approaches.
- Schools and colleges should be aware of how to respond appropriately to incidents involving harmful online challenges and online hoaxes. DSLs and SLT should access the DfE guidance to help ensure they are prepared in advance of any concerns locally or nationally. Additionally, the following links may also be helpful:
    - The Education People: Think before you scare
    - UK Safer Internet Centre: De-escalating and responding to harmful online challenges
    - London Grid for Learning: Parents – scare or prepare?
- One-off events, lessons or assemblies or a reliance on external speakers, are not effective or adequate practice to ensure a robust approach to online safety education. External speakers can be useful as a catalyst to a discussion or to reinforce learning but are unlikely to be successful if they are the sole source of education or sanctions; in some cases, this approach can undermine the school/college ability to develop internal capacity to respond to concerns.
    - UKCIS have published guidance for educational settings regarding the use of external visitors.

Action points:

- How does your school/college teach children about online safety?
    - Have staff (subject leads, class teachers etc.) read and implemented guidance and appropriate curriculum resources in accordance with your local context?
    - Are all children receiving up-to-date education that is relevant to their age and?
    - Is there a clear RSE approach in place which uses relevant and appropriate teaching resources?
- Are staff familiar with the resources identified in paragraphs 133 and 134?
- How does your school/college identify and target vulnerable children who may require a more specific and adapted/targeted education to enable them to build online safety skills?
- How are children and young people involved in the development of the curriculum?
- Is the curriculum integrated throughout the year and across different subject areas?
- How does your school/college use external speakers to complement internal education approaches?

134. Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.

Practice Implications

- Governing bodies and proprieties should be aware of 'appropriate filtering and monitoring' approaches in place and consider how their settings can evidence reasonable restrictions are in place.

Online Safety within 'Keeping Children Safe in Education' 2023

Online safety

135. 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.

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

- Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- 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.
- 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
- Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)

137. Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.

Practice Implications

- Online safety should be viewed as part of your school and college safeguarding responsibilities; we need to ensure that all members of our community develop appropriate understanding and skills to prepare them to respond to online safety issues.
    - The advice given by the school or college should empower their community to be able to respond to a range of online risks as well as recognising the opportunities technology brings.
- Settings should develop and implement a curriculum, appropriate to the needs of their learners, which covers the range of online safety issues identified above.
- Paragraph 137 references the responsibility for governing bodies and proprietors to ensure online safety is embedded a long-term whole school/college approach and should not be viewed as a one-off 'tick box' input or event.
    - Online safety messages shared with staff and parents/carers should be appropriate and up-to-date and reflect the full range of risks children and young people could encounter online; content, contact, conduct and commerce.
    - Schools/colleges should consider how they engage parents/carers; this is an ongoing task and will require a range of different approaches. This will vary from setting to setting but

could include raising awareness via targeted events, learner led education and regular communication, for example, newsletters and social media.
    - Schools and colleges should make informed decisions about any resources they use with parents/carers. We suggest using resources from known and recognised organisations, for example, NSPCC, NCA-CEOP, Childnet, Internet Matters etc.
    - Additional information can be found on our blog post 'Online Safety FAQ - How can we get families more involved in Online Safety?'
    - Where specific online safeguarding issues involving learners are identified, schools and colleges should ensure they work directly with families involved and action is taken in line with safeguarding policies.
    - Where there are concerns regarding harmful challenges and hoaxes circulating online, schools and colleges should follow the DfE Harmful online challenges and online hoaxes guidance.

Action points:

- Are staff aware of the 4 C's: content, contact and conduct?
- Does the online safety curriculum cover the full range of potential online risks which children may encounter?

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.

Practice Implications

- **Update:** Para 138 has been updated to clarify that the school/college child protection policies should specifically address appropriate filtering and monitoring on school devices and school networks.
- Online safety should be clearly referenced as part of the school/college child protection policy; many schools and colleges opt to have a standalone online safety policy; itis not a statutory requirement to have a separate policy and this is a decision individual school/college leadership teams should make depending on their specific context.
    - Some schools/colleges prefer to keep all online safety related information in one place, others prefer to incorporate it within existing policies. We suggest that key online elements (such as child-on-child abuse, filtering and monitoring, social media, and use of mobile

technology) should be addressed within your child protection policy or other relevant safeguarding policies if online safety is not addressed in a standalone policy.
    - Whichever approach schools/colleges take, all policies should be up to date (reviewed at least annually) and appropriately cross referenced with other relevant policies.
- Schools and colleges should have a clear policy regarding decisions with regards to the use of mobile and smart technology for example, wearable technology. The policy should specifically address how personal use of mobile and smart technology will be managed on site.
    - The Education Safeguarding Service provide child protection, social media and mobile and smart technology policy templates which schools and colleges can adapt; our child protection policy has a specific section regarding appropriate filtering and monitoring for schools/colleges to adapt.
    - Schools who are members of the Education Safeguarding Support Package have access to an online safety policy template. The online safety policy template, along with additional guidance and our anti-bullying policy template are available to purchase standalone.

Action points:

- Where is online safety addressed in your school/college policies? For example, is it addressed in your child protection policy, or do you also have a standalone online safety policy?
    - If you have a standalone policy, is it up to date (reviewed at least annually) and available publicly? Is it cross referenced with your child protection policy?
- Does your policy include appropriate filtering and monitoring on school devices and school networks?
- Do your policies clearly reflect any actual practice decisions and expectations?
- Do your policies reflect your local context, for example, is it appropriate to the age/ability of your learners and any technology use?
- Does the setting have a clear policy regarding the use of mobile and smart technology on premises, including phones and other personal devices?
- How are your policies communicated to staff, learners, and parents/carers?

Remote learning

139. Guidance to support schools and colleges understand how to help keep pupils, students and staff safe whilst learning remotely can be found at https://www.gov.uk/guidance/safeguarding-and-remote-education and https://www.gov.uk/government/publications/providing-remote-education-guidance-for-schools. The NSPCC also provide helpful advice - Undertaking remote teaching safely.

140. Schools and colleges are likely to be in regular contact with parents and carers. Those communications should be used to reinforce the importance of children being safe online and parents and carers are likely to find it helpful to understand what systems schools and colleges use to filter and monitor online use. It will be especially important for parents and carers to be aware of what their children are being asked to do online, including the sites they will asked to access and be clear who from the school or college (if anyone) their child is going to be interacting with online.

Online Safety within 'Keeping Children Safe in Education' 2023

Practice Implications

- Paragraph 139 provides links to specific remote learning guidance from the DFE and NSPCC.
- The Education Safeguarding Service have published guidance and templates for educational settings to use following Covid-19 restrictions. A remote learning AUP is also included within our AUP templates.

Action points:

- Have you accessed the national/local guidance regarding remote learning and implemented appropriate boundaries and expectations regarding safer use?
    - How do you evidence this is in place? For example, risk assessments, updated AUPs etc.
- How do you evidence communication with parents/carers to reinforce the importance of children being safe online and sharing understand what systems are used to filter and monitor online use?
- Have you informed parents/carers of what their children are being asked to do online, including the sites they will be asked to access, and who from the school/college (if anyone) their child is going to be interacting with online?
    - How do you evidence this is in place? For example, risk assessments, communication on your website, updated AUPs etc.

Filters 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.

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.

Online Safety within 'Keeping Children Safe in Education' 2023

Additional guidance on filtering and monitoring can be found at: UK Safer Internet Centre: "appropriate" filtering and monitoring. https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring. South West 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).

143. Support for schools when considering what to buy and how to buy it is available via the: schools' buying strategy with specific advice on procurement here: buying for schools.

Practice Implications

- **Paragraph 141 has been updated** to identify that governing bodies and proprietors should consider those children who are potentially at greater risk of harm when making decision relating to filtering and monitoring approaches.
- Governing bodies and proprietors should make informed decisions regarding the safety and security of the internet access and equipment available within or provided by their school or college. The welfare of children and young people is paramount, and any decisions taken regarding filtering and monitoring systems should be taken from a safeguarding, educational and technical approach; flirting and monitoring decisions should be justifiable and documented.
    - The UK Safer internet Centre provide guidance about appropriate filtering and monitoring: UK Safer Internet Centre: appropriate filtering and monitoring. It is recommended that governing bodies, proprietors, headteachers and DSLs read and consider this guidance when considering their filtering and monitoring systems and any associated decisions.
    - When reviewing filtering and monitoring system options and approaches, schools/colleges may wish to undertake an approach which includes robust risk assessments and a through comparison which identify both the benefits and limitations of the services
    - Schools/colleges could approach their broadband provider to consider the range of tools available that may enable them to develop strategies to control and supervise their internet use and systems appropriately.
    - The UK Safer Internet Centre website contains a number of provider responses from popular services used by schools to provide filtering and monitoring solutions.
    - The SWGfL 'Test Filtering' tool allows schools and colleges to check their Internet Service Providers filtering approaches.
    - Schools who are members of the Education Safeguarding Support Package have access to our 'filtering and monitoring considerations for school leaders and governors' document.
- **Paragraph 142 has been updated** to add a new section referencing the DfE filtering and monitoring standards: The standards are to support schools meet their duty to have appropriate/effective filtering and monitoring systems in place, and is not a new burden
- No filtering or monitoring solution can offer educational settings 100% protection from exposure to inappropriate or illegal content, so it is important they can demonstrate they have taken all other reasonable precautions. A reliance on filtering and monitoring to safeguarding children online could lead to a feeling of complacency and can put children and adults at risk of significant harm. Suggestions of this can include appropriate supervision, implementing Acceptable Use Policies (AUP), implementing a robust and embedded online safety curriculum and providing staff training etc.

Online Safety within 'Keeping Children Safe in Education' 2023

Action points:

- Has the leadership accessed the appropriate guidance regarding filtering and monitoring guidance/, for example from the DfE, the UK Safer Internet centre and any local guidance/support?
- What evidence is there that the school/college is meeting the DfE filtering and monitoring standards?
    - Has the school/college identified and assigned roles and responsibilities to manage filtering and monitoring systems?
    - How does the school/college review filtering and monitoring provision at least annually?
    - How does the school college ensure the filtering system blocks harmful and inappropriate content without unreasonably impacting teaching and learning?
    - How does the school implement effective monitoring strategies in place that meet their safeguarding needs?
- Does the leadership team have an awareness and understanding of the current filtering/monitoring systems in place?
    - Do they manage them effectively and know how to escalate concerns when identified? If not, how can this be developed?
- How has the governing body/proprietor made informed decisions regarding the school/college filtering and monitoring systems and associated decisions? How is this decision making evidenced?
- How do the governing body/proprietor ensure the school/college is regularly reviewing the effectiveness of filtering and monitoring systems?
- How is information about filtering and monitoring shared with the community? For example, is filtering and monitoring explicitly covered within staff training, the child protection policy and/or any AUPs?
- How do SLT work with the IT service providers/staff (for example your broadband provider, IT Technicians, Network Managers, or external IT service providers) to implement filtering and monitoring decisions and act on concerns identified? How is this evidenced?
- How do all members of staff ensure that technology in the classroom is used as safely and effectively?
    - Does the setting provide all members of staff with clear expectations regarding use of technology, for example, supervision, pre-checking content before use, use of age-appropriate tools, understanding of data protection concerns, clear risk assessments etc.

Information security and access management

143. Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place, in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. Guidance on e-security is available from the National Education Network. In addition, schools and colleges should consider meeting the Cyber security standards for schools and colleges.GOV.UK. Broader guidance on cyber security including considerations for governors and trustees can be found at Cyber security training for school staff - NCSC.GOV.UK.

Online Safety within 'Keeping Children Safe in Education' 2023

Practice Implications

- **Paragraph 143 has been updated** to add a new section referencing the DfE cyber security standards: The standards are to support schools meet their duty to have appropriate approaches towards cyber security in place and is not a new burden.
- School and college leaders should work with their DSLs and technical staff/support to ensure appropriate security protection procedures are in place to safeguard their systems and community. The specific approaches required will vary but are likely to depend on technology use and access and learners age and ability.
- Decisions should be documented within appropriate policies, for example AUPs, standalone IT security policies etc. but should be shared with the community as appropriate.

Action points:

- What evidence is there that the school/college is meeting the DfE cyber security standards?
- How does the school/college leadership work with and support technical staff to implement robust security protection procedures?
- How are expectations communicated to staff, learners, and parents/carers?
    - Have all staff with access to school/college networks had basic cyber security training as a minimum?

Reviewing online safety

145. Technology, and risks and harms related to it evolve and changes rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. A free online safety self-review tool for schools can be found via the 360 safe website or LGfL online safety audit.

146. UKCIS has published Online safety in schools and colleges: Questions from the governing board. The questions can be used to gain a basic understanding of the current approach to keeping children safe online; learn how to improve this approach where appropriate; and find out about tools which can be used to improve the approach. It has also published an Online Safety Audit Tool which helps mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring.

147. When reviewing online safety provision, the UKCIS external visitors guidance highlights a range of resources which can support educational settings to develop a whole school approach towards online safety.

Practice Implications

- School and college leaders should carry out an annual review of their approach to online safety, supported by an annual risk assessment which considers and reflects the risks their learners face.
    - In additional to the 360 safe or LGFL audit tool, Schools who are members of the Education Safeguarding Support Package have access to an online safety self-review tool.

Online Safety within 'Keeping Children Safe in Education' 2023

Action points:

- Has your school/college carried out an annual review of your approach to online safety, supported by an annual risk assessment that considers and reflects the specific risks your children face?
- How do you evidence that your school/college is reviewing its online safety practice regularly and making changes as required?

Information and support

148. There is a wealth of additional information available to support schools, colleges and parents to keep children safe online. A sample is provided at Annex B.

Practice Implications

- The guidance in annex B links to a range of updated sources of support and resources.
    - The Education Safeguarding Service provide specialist online safety advice, training, and guidance to educational settings in Kent.
    - Local information about online safety is provided for DSLs through the Education Safeguarding Service Child Protection Newsletter, and Kent Online Safety Twitter feed.

Action points:

- How does your school/college (especially the DSL) evidence they are keeping up to date with developments within the online safety agenda?

Child-on-child abuse

156. All staff should recognise that children are capable of abusing other children (including online). All staff should be clear about their school's or college's policy and procedures with regard to child-on-child abuse.

157. Governing bodies and proprietors should ensure that their child protection policy includes:

- procedures to minimise the risk of child-on-child abuse
- the systems in place (and they should be well promoted, easily understood and easily accessible) for children to confidently report abuse, knowing their concerns will be treated seriously
- how allegations of child-on-child abuse will be recorded, investigated, and dealt with
- clear processes as to how victims, perpetrators and any other children affected by child-on-child abuse will be supported
- a recognition that even if there are no reported cases of child-on-child abuse, such abuse may still be taking place and is simply not being reported
- a statement which makes clear there should be a zero-tolerance approach to abuse, and it should never be passed off as "banter", "just having a laugh", "part of growing up" or "boys being boys" as this can lead to a culture of unacceptable behaviours and an unsafe environment for children
- recognition that it is more likely that girls will be victims and boys' perpetrators, but that all child-on-child abuse is unacceptable and will be taken seriously, and
- the different forms child-on-child abuse can take, such as:

- bullying (including cyberbullying, prejudice-based and discriminatory bullying)
  - abuse in intimate personal relationships between children (also known as teenage relationship abuse)
  - physical abuse which can include hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm
  - sexual violence and sexual harassment. Part five of this guidance sets out how schools and colleges should respond to reports of sexual violence and sexual harassment
  - consensual and non-consensual sharing of nude and semi-nude images and/or videos (also known as sexting or youth produced sexual imagery): the policy should include the school or college's approach to it. The Department provides Searching Screening and Confiscation Advice for schools. The UKCIS Education Group has published Sharing nudes and semi-nudes: advice for education settings working with children and young people which outlines how to respond to an incident of nude and/or semi-nude being shared
  - causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
  - upskirting (which is a criminal offence), which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress, or alarm, and
  - initiation/hazing type violence and rituals.

Practice Implications

- The UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' guidance was published in December 2020 and replaced the previous 'sexting in schools' guidance.
- We recommend all DSLs are familiar with this content as it will support them in responding effectively to incidents involving the sharing of nudes and semi-nudes by children and young people. UKCIS also provide a single page summary which DSLs may find helpful to share with staff.

Action points:

- Do all staff recognise that children can abuse other children online? How do you know this is achieved?
- Does your child protection policy clearly identify policies and procedures to follow when responding to online child-on-child abuse concerns, for example, consensual and non-consensual sharing of nudes and semi-nude images and/or videos?

Children potentially at greater risk of harm

Children with special educational needs, disabilities or health issues

199. Children with special educational needs or disabilities (SEND) or certain medical or physical health conditions can face additional safeguarding challenges both online and offline. Governing bodies and

proprietors should ensure their child protection policy reflects the fact that additional barriers can exist when recognising abuse and neglect in this group of children. These can include:

- assumptions that indicators of possible abuse such as behaviour, mood and injury relate to the child's condition without further exploration
- these children being more prone to peer group isolation or bullying (including prejudice-based bullying) than other children
- the potential for children with SEND or certain medical conditions being disproportionately impacted by behaviours such as bullying, without outwardly showing any signs, and
- communication barriers and difficulties in managing or reporting these challenges. • cognitive understanding – being unable to understand the difference between fact and fiction in online content and then repeating the content/behaviours in schools or colleges or the consequences of doing so.

200. Any reports of abuse involving children with SEND will therefore require close liaison with the designated safeguarding lead (or a deputy) and the SENCO or the named person with oversight for SEND in a college.

201. Schools and colleges should consider extra pastoral support and attention for these children, along with ensuring any appropriate support for communication is in place.

Children who are lesbian, gay, bi, or trans (LGBT)

203. The fact that a child or a young person may be LGBT is not in itself an inherent risk factor for harm. However, children who are LGBT can be targeted by other children. In some cases, a child who is perceived by other children to be LGBT (whether they are or not) can be just as vulnerable as children who identify as LGBT.

204. Risks can be compounded where children who are LGBT lack a trusted adult with whom they can be open. It is therefore vital that staff endeavour to reduce the additional barriers faced and provide a safe space for them to speak out or share their concerns with members of staff.

205. LGBT inclusion is part of the statutory Relationships Education, Relationship and Sex Education and Health Education curriculum and there is a range of support available to help schools counter homophobic, biphobic and transphobic bullying and abuse.

Practice Implications

- Children with special educational needs, disabilities or health issues, or those who are LGBT or are perceived as LGBT can be at increased risk online. DSLs are likely to require additional knowledge to support learners who are potentially at greater risk of harm online and will need to work with specialist staff as appropriate.

Online Safety within 'Keeping Children Safe in Education' 2023

Part three: Safer Recruitment

221. In addition, as part of the shortlisting process schools and colleges should consider carrying out an online search as part of their due diligence on the shortlisted candidates. This may help identify any incidents or issues that have happened, and are publicly available online, which the school or college might want to explore with the applicant at interview. Schools and colleges should inform shortlisted candidates that online searches may be done as part of due diligence checks. See Part two - Legislation and the Law for information on data protection and UK GDPR.

Practice Implications

- KCSIE is not prescriptive in detailing the way 'online searches' should be undertaken but according to the DfE, care has been taken not to use the term 'social media,' as this could be seen as invasive. KCSIE requests that schools and colleges consider an 'online search' which should be a quick and simple search, and can be conducted, for example via an internet browser. The guidance should not place any unnecessary burdens on schools and colleges, nor encourage them to breach any individual's private life.
- Where schools and colleges opt to carry online searches on shortlisted candidates, this should be done so safely and effectively, for example, only accessing content that is available publicly and in line with appropriate privacy and data protection legislation. Paragraph 221 has been updated to clarify that searches should be transparent and shortlisted candidates should be informed online searches may be undertaken as part of due diligence checks.
- Schools/colleges should ensure they have a process to follow if they identify something that is significantly concerning, for example something that could indicate a candidate is unsuitable to work with children.
- We recommend this is addressed in any safer recruitment policies and schools/college may also wish to seek specialist advice from their HR/personnel provider.

Action points:

- If we undertake online searches as part of due diligence checks on shortlisted candidates, are these carried out safety and transparently?

Part four: Safeguarding concerns and allegations made about staff, including supply teachers, volunteers and contractors

352. Schools and colleges should have their own procedures for dealing with safeguarding concerns or allegations against those working in or on behalf of schools and colleges in a paid or unpaid capacity, this includes, members of staff, supply teachers, volunteers and contractors.

353. This part of the guidance has two sections covering the two levels of allegation/concern:

1. Allegations that may meet the harm threshold.
2. Allegations/concerns that do not meet the harm threshold – referred to for the purposes of this guidance as 'low-level concerns'.

Practice Implications

- It is important to acknowledge that the guidance in both section one and two can apply to concerns about staff behaviour online as well as offline.

What is a low-level concern?

426. The term 'low-level' concern does not mean that it is insignificant. A low-level concern is any concern – no matter how small, and even if no more than causing a sense of unease or a 'nagging doubt' - that an adult working in or on behalf of the school or college may have acted in a way that:

- is inconsistent with the staff code of conduct, including inappropriate conduct outside of work and
- does not meet the harm threshold or is otherwise not serious enough to consider a referral to the LADO.

Examples of such behaviour could include, but are not limited to:

- being over friendly with children
- having favourites
- taking photographs of children on their mobile phone, contrary to school policy
- engaging with a child on a one-to-one basis in a secluded area or behind a closed door, or
- humiliating children.

Practice Implications

- The section includes updated examples of low-level concerns, including an example involving the use of technology.

Action points:

- Do your school/college policies make it clear that allegations that may meet the harm threshold and 'low-level concerns' can apply to concerns regarding the use of technology and staffs online conduct, both on and offsite?

Part five: Child on child sexual violence and sexual harassment

446. This part of the statutory guidance is about how schools and colleges **should respond to all signs, reports and concerns** of child-on-child sexual violence and sexual harassment, including those that have happened outside of the school or college premises, and/or online (what to look out for and indicators of abuse are set out in Part one of this guidance). As set out in Part one of this guidance, all staff working with children are advised to maintain an attitude of 'it could happen here', and this is especially important when considering child-on-child abuse.

Practice Implications

- It should be assumed that where the guidance addresses child-on-child sexual violence and harassment, it also includes cases where that behaviour/abuse takes place online. This document will focus on where online is specifically mentioned.

Online Safety within 'Keeping Children Safe in Education' 2023

What schools and colleges should be aware of

447. Sexual violence and sexual harassment can occur between two or more children of any age and sex, from primary through to secondary stage and into college. It can occur also through a group of children sexually assaulting or sexually harassing a single child or group of children. Sexual violence and sexual harassment exist on a continuum and may overlap; they can occur online and face-to-face (both physically and verbally) and are never acceptable. Schools and colleges should be aware of the importance of:

- making clear that there is a zero-tolerance approach to sexual violence and sexual harassment, that it is never acceptable, and it will not be tolerated. It should never be passed off as "banter", "just having a laugh", "a part of growing up" or "boys being boys". Failure to do so can lead to a culture of unacceptable behaviour, an unsafe environment and in worst case scenarios a culture that normalises abuse, leading to children accepting it as normal and not coming forward to report it
- recognising, acknowledging, and understanding the scale of harassment and abuse and that even if there are no reports it does not mean it is not happening, it may be the case that it is just not being reported
- challenging physical behaviour (potentially criminal in nature) such as grabbing bottoms, breasts and genitalia, pulling down trousers, flicking bras and lifting up skirts. Dismissing or tolerating such behaviours risks normalising them

449. Whilst any report of sexual violence or sexual harassment should be taken seriously, staff should be aware it is more likely that girls will be the victims of sexual violence and sexual harassment and more likely it will be perpetrated by boys. Children with special educational needs and disabilities (SEND) are also three times more likely to be abused than their peers.

450. Ultimately, it is essential that all victims are reassured that they are being taken seriously and that they will be supported and kept safe.

Practice Implications

- Schools and colleges should be mindful that sexual violence or harassment can occur online and can be concurrent with offline behaviour.
- Children may feel less likely to report online sexual violence/harassment due to fear of being punished or blamed, therefore schools/colleges should ensure their learners and staff are aware of your expectations and approaches.

Sexual violence

451. It is important that schools and colleges are aware of sexual violence and the fact children can, and sometimes do, abuse other children in this way and that it can happen **both inside and outside of school/college**. When referring to sexual violence in this advice, we do so in the context of child-on-child sexual violence.

Practice Implications

- It is important to acknowledge the role technology may have to play in facilitating sexual violence – for example a sexual assault could be videoed and distributed online.

Sexual harassment

452. When referring to sexual harassment we mean 'unwanted conduct of a sexual nature' that can occur online and offline and both inside and outside of school/college. When we reference sexual harassment, we do so in the context of child-on-child sexual harassment. Sexual harassment is likely to: violate a child's dignity, and/or make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

453. Whilst not intended to be an exhaustive list, sexual harassment can include: …

- …displaying pictures, photos or drawings of a sexual nature
- upskirting (this is a criminal offence), and
- online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:
    - consensual and non-consensual sharing of nude and semi-nude images and/or videos. Taking and sharing nude photographs of U18s is a criminal offence. UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people provides detailed advice for schools and colleges.
    - sharing of unwanted explicit content
    - sexualised online bullying
    - unwanted sexual comments and messages, including, on social media
    - sexual exploitation; coercion and threats, and
    - coercing others into sharing images of themselves or performing acts they're not comfortable with online.

453. It is important that schools and colleges consider sexual harassment in broad terms. Sexual harassment (as set out above) creates a culture that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence.

Practice Implications

- It is important to acknowledge the role technology may have to play in sexual harassment and the importance of schools/colleges responding appropriately, even if this behaviour is taking place offsite.

Harmful sexual behaviour

455. Children's sexual behaviour exists on a wide continuum, ranging from normal and developmentally expected to inappropriate, problematic, abusive and violent. Problematic, abusive and violent sexual behaviour is developmentally inappropriate and may cause developmental damage. A useful umbrella term is "harmful sexual behaviour" (HSB). The term has been widely adopted in child protection and is used in

this advice. **HSB can occur online and/or face-to-face and can also occur simultaneously between the two**. HSB should be considered in a child protection context.

Responding to reports of sexual violence and sexual harassment

Support for schools and colleges

465. Schools and colleges should not feel that they are alone in dealing with sexual violence and sexual harassment

466. Local authority children's social care and the police will be important partners where a crime might have been committed. Referrals to the police will often be a natural progression of making a referral to local authority children's social care. The designated safeguarding lead (or a deputy) should lead the school or college response and should be aware of the local process for referrals to children's social care and making referrals to the police (also see the section "reporting to the police" on page 119 for further information). Schools and colleges may also find the following resources helpful: …

- National Crime Agency's CEOP Safety Centre: The CEOP Safety Centre aims to keep children and young people safe from online sexual abuse. Online sexual abuse can be reported on their website and a report made to one of its Child Protection Advisors.
- The NSPCC provides a helpline for professionals at 0808 800 5000 and help@nspcc.org.uk. The helpline provides expert advice and support for school and college staff and will be especially useful for the designated safeguarding lead (and their deputies)
- Support from specialist sexual violence sector organisations such as Rape Crisis or The Survivors Trust
- The Anti-Bullying Alliance has developed guidance for schools about Sexual and sexist bullying.

Online: Schools and colleges should recognise that sexual violence and sexual harassment occurring online (either in isolation or in connection with face-to-face incidents) can introduce a number of complex factors. Amongst other things, this can include widespread abuse or harm across a number of social media platforms that leads to repeat victimisation. Online concerns can be especially complicated and support is available from:

- The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. The helpline provides expert advice and support for school and college staff with regard to online safety issues
- Internet Watch Foundation: If the incident/report involves sexual images or videos that have been made and circulated online, the victim can be supported to get the images removed by the Internet Watch Foundation (IWF)
- Childline/IWF Report Remove is a free tool that allows children to report nude or sexual images and/or videos of themselves that they think might have been shared online

- UKCIS Sharing nudes and semi-nudes advice: Advice for education settings working with children and young people on responding to reports of children sharing non-consensual nude and semi-nude images and/or videos (also known as sexting and youth produced sexual imagery).
- National Crime Agency's CEOP Education Programme provides information for the children's workforce and parents and carers on protecting children and young people
- from online child sexual abuse.
- LGFL 'Undressed' provides schools advice about how to teach young children about being tricked into getting undressed online in a fun way without scaring them or explaining the motives of sex offenders.

Additional sources of support are listed at the end of Annex B.

Practice Implications

- Schools/colleges should recognise their role in responding to online sexual violence and sexual harassment. Staff should be aware it can occur in isolation or in connection with face-to-face incidents and can introduce a number of complicating factors, for example sharing rumours or content over social media leading to repeat victimisation. The guidance signposts to a number of national support organisations.
- The Education Safeguarding Service provide specialist online safety advice, training and guidance to educational settings in Kent.

Action points:

- Are all your DSLs (and staff as appropriate) aware of the online safety support/organisations listed in KCSIE; specifically, those mentioned in part five and annex B?
- Are all your DSLs (and their staff as appropriate) aware of any local support available to assist schools/colleges in preventing and responding to online safety concerns?

The immediate response to a report

Responding to the report

470. As per Part one of this guidance, all staff should be trained to manage a report. Local policies (and training) will dictate exactly how reports should be managed. However, effective safeguarding practice includes: …

- careful management and handling of reports that include an online element. Including being aware of searching screening and confiscation advice (for schools) and UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people. **The key consideration is for staff not to view or forward illegal images of a child.** The highlighted advice provides more details on what to do when viewing an image is unavoidable. In some cases, it may be more appropriate to confiscate any devices to preserve any evidence and hand them to the police for inspection

Practice Implications

- The term 'sharing nudes and semi-nudes' is used to mean the sending or posting of nude or semi-nude images, videos or live streams of/by young people under the age of 18 online. Many professionals refer to 'nudes and semi-nudes' as youth produced sexual imagery or 'youth involved'

sexual imagery, indecent imagery (the legal term used to define nude or semi-nude images and videos of children and young people under the age of 18), 'sexting', or image-based sexual abuse.

- Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents complex. There are also a range of risks which need careful management from those working in education settings.
    - The UKCIS advice outlines how DSLs should respond to incidents of nude and semi-nude images or videos being shared. This includes risk assessing situations, effectively safeguarding and supporting children and young people, handling devices and images including viewing/deleting imagery, the role of other agencies (such as when schools and colleges should involve police and/or children social care) and working with parents and carers.
    - The types of incidents covered in the UKCIS advice are a person under the age of 18 creates and shares nudes and semi-nudes of themselves with a peer under the age of 18; a person under the age of 18 shares nudes and semi-nudes created by another person under the age of 18 with a peer under the age of 18; and a person under the age of 18 is in possession of nudes and semi-nudes created by another person under the age of 18.
- The UKCIS advice does not cover the sharing of nudes and semi-nudes of under 18s by adults (18 and over) as this constitutes child sexual abuse and education settings should always inform their local police force as a matter of urgency; or children and young people under the age of 18 sharing adult pornography or exchanging sexualised texts which do not contain images. Schools and colleges should respond to these child-on-child concerns in line with existing policies, for example their child protection, mobile technology and behaviour policies.
- Schools/colleges should ensure there is a policy in place which clearly details expectations and procedures to follow with regards to confiscation of and searching of devices, including non-school owned devices.

Action points:

- Have all DSLs read and understood the UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people guidance?
- Has information been shared with all staff regarding procedures to follow when responding to nude and semi-nude image sharing concerns?
- Is there a policy in place which clearly sets out your procedures and expectations with regards to searching, screening and confiscation of devices?

Anonymity

479. Schools and colleges should also consider the potential impact of social media in facilitating the spreading of rumours and exposing victims' identities. The unique challenges regarding social media are discussed at paragraph 466 along with potential support. In addition, the principles described in Childnet's cyberbullying guidance could be helpful.

Practice Implications

- Schools/colleges should recognise the impact and complications social media can bring when responding child on child sexual violence and harassment concerns. In addition to the organisations

listed in paragraph 466, the Education Safeguarding Service provide specialist online safety advice, training and guidance specifically for educational settings in Kent.

Action points:

- When responding to child-on-child sexual violence and harassment concerns, do all DSLs consider the potential impact of social media?
- Are all your DSLs (and their staff as appropriate) aware of any national and local support available to assist schools/colleges in preventing and responding to online safety concerns?

Action following a report of sexual violence and/or sexual harassment

What to consider

483. As set out above, sexual violence and sexual abuse can happen anywhere, and all staff working with children are advised to maintain an attitude of '**it could happen here'**. Schools and colleges should be aware of and respond appropriately to **all** reports and concerns about sexual violence and/or sexual harassment both online and offline, including those that have happened outside of the school/college. The designated safeguarding lead (or deputy) is likely to have a complete safeguarding picture and be the most appropriate person to advise on the initial response by the school or college.…

Practice Implications

- This will include where sexual violence or harassment takes places online or is facilitated by digital technology, for example an offline issue is shared/discussed in an online context.
- All reports and concerns about sexual violence and/or sexual harassment online should be reported to the DSL (or an appropriately trained deputy).

Action points:

- Are all reports and concerns about online sexual violence and/or sexual harassment reported to the DSL or an appropriately trained deputy?

Ongoing response

Safeguarding and supporting the victim

532. Support can include: …

- Childline provides free and confidential advice for children and young people.
- Internet Watch Foundation works internationally to remove child sexual abuse online images and videos and offers a place for the public to report them anonymously.
- Childline / IWF: Remove a nude image shared online Report Remove is a free tool that allows children to report nude or sexual images and videos of themselves that they think might have been shared online, to see if they can be removed from the internet.

538. It is important that the school or college do everything they reasonably can to protect the victim from bullying and harassment as a result of any report they have made.

Practice Implications

- This should include online harassment and cyberbullying.

Safeguarding and supporting the alleged perpetrator(s) and children and young people who have displayed harmful sexual behaviour

541. The following principles are based on effective safeguarding practice and should help shape any decisions regarding safeguarding and supporting the alleged perpetrator(s): …

- The Lucy Faithfull Foundation has developed a HSB toolkit, which amongst other things, provides support, advice and information on how to prevent it, links to organisations and helplines, resources about HSB by children, internet safety, sexual development and preventing child sexual abuse…

Safeguarding other children

555. Social media is very likely to play a central role in the fall out from any incident or alleged incident. There is the potential for contact between victim and alleged perpetrator(s) and a very high likelihood that friends from either side could harass the victim or alleged perpetrator(s) online and/or become victims of harassment themselves. Specialist online safety support is discussed at page 110.

Action points:

- Are all your DSLs (and staff as appropriate) aware of the online safety support/organisations listed in KCSIE (part five and annex B)?
- Are all your DSLs (and their staff as appropriate) aware of any local support available to assist schools/colleges in safeguarding victims, alleged perpetrators, and other children online?

Annex B: Further information

Practice Implications

- Annex B contains important additional information about specific forms of abuse and safeguarding issues. School and college leaders and those staff who work directly with children should read annex B.
- The following information is where forms of abuse listed in annex B specifically include references to technology and/or online behaviour or risks.

Child Criminal Exploitation (CCE) and Child Sexual Exploitation (CSE)

Some of the following can be indicators of both child criminal and sexual exploitation where children:

- appear with unexplained gifts, money or new possessions…

County lines

County lines is a term used to describe gangs and organised criminal networks involved in exporting illegal drugs using dedicated mobile phone lines or other form of "deal line". This activity can happen locally as well as across the UK - no specified distance of travel is required. Children and vulnerable adults are

exploited to move, store and sell drugs and money. Offenders will often use coercion, intimidation, violence (including sexual violence) and weapons to ensure compliance of victims….. Children are also increasingly being targeted and recruited online using social media…

Practice Implications

- This can involve new access to technology, for example brand new smart phones or other devices such as smart watches.
    - This identifies the role social media can play in facilitating CCE.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include:

- unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded
- denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above

Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Note that Cyber Choices does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

Additional advice can be found at: Cyber Choices, 'NPCC- When to call the Police' and National Cyber Security Centre.

Practice Implications

- This section was added to annex B in 2021.
- Whilst it is likely cyber security education will be delivered within the computing curriculum, cybercrime issues involving learners should be recognised by schools and colleges as a safeguarding concern.

- Whilst some content will be covered with school and colleges IT security policies, cybercrime should also be addressed or referenced within school/college child protection and safeguarding policies and procedures.
- Cyber Choices does not cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs, child sexual abuse and exploitation, or other areas of concern such as cyberbullying.
- Local support is also likely to be available to schools and colleges via police forces, for example via Kent Police.

Domestic abuse

The Domestic Abuse Act 2021 received Royal Assent on 29 April 2021. The Act introduces the first ever statutory definition of domestic abuse and recognises the impact of domestic abuse on children, as victims in their own right, if they see, hear or experience the effects of abuse. The statutory definition of domestic abuse, based on the previous cross-government definition, ensures that different types of relationships are captured, including ex-partners and family members. The definition captures a range of different abusive behaviours, including physical, emotional and economic abuse and coercive and controlling behaviour. Under the statutory definition, both the person who is carrying out the behaviour and the person to whom the behaviour is directed towards must be aged 16 or over and they must be "personally connected" (as defined in section 2 of the 2021 Act).

Types of domestic abuse include intimate partner violence, abuse by family members, teenage relationship abuse and child/adolescent to parent violence and abuse. Anyone can be a victim of domestic abuse, regardless of sexual identity, age, ethnicity, socioeconomic status, sexuality or background and domestic abuse can take place inside or outside of the home…

… Young people can also experience domestic abuse within their own intimate relationships. This form of child-on-child abuse is sometimes referred to as 'teenage relationship abuse'. Depending on the age of the young people, this may not be recognised in law under the statutory definition of 'domestic abuse' (if one or both parties are under 16). However, as with any child under 18, where there are concerns about safety or welfare, child safeguarding procedures should be followed and both young victims and young perpetrators should be offered support.

Practice Implications

- The definition of domestic abuse now captures a range of different abusive behaviours, including physical, emotional, and economic abuse and coercive and controlling behaviour. It is important to recognise that technology can be a tool to facilitate domestic abuse, for example 'cyberstalking', covertly monitoring online activity, using GPS tracking etc. and this can take place as part of 'teenage relationship abuse'. A key response to tackling 'teenage relationship abuse' will be in the school/college RSE approaches.
- Although aimed at safeguarding individuals over 18 and not covered within KCISE, it is also important for schools and colleges to be aware that the Domestic Abuse Act also included extension to so called 'Revenge Porn' laws.
    - From 29th June 2021, it became an offence not just to disclose, but to threaten to disclose private sexual photographs or films in which another individual appears, if it is done with the intent to cause distress to that individual, and if the disclosure is, or would be, made without

the consent of that individual. It is not necessary for any prosecution to prove that the photograph or film referred to in the threat exists. If a film or photograph does exist, the prosecution will not have to prove that is it a private sexual photograph or film.

Mental health

Where children have suffered abuse and neglect, or other potentially traumatic adverse childhood experiences, this can have a lasting impact throughout childhood, adolescence and into adulthood. It is key that staff are aware of how these children's experiences, can impact on their mental health, behaviour, attendance and progress at school.

Practice Implications

- Whilst the online space is not mentioned explicitly, it is important to recognise the role social media can play as part of children and young people's mental health. Which research is often conflicting, it should be recognised that social media can have positive and negative impacts on young people's social media use; it is important for education professionals to be curious about children's use of social media and provide balanced education to promote safe and healthy use.
- Where schools/colleges are concerned about the impact of technology on young people's mental health, they should seek appropriate advice and support as they would offline concerns.

Preventing radicalisation

Children are vulnerable to extremist ideology and radicalisation. Similar to protecting children from other forms of harms and abuse, protecting children from this risk should be a part of a schools' or colleges' safeguarding approach…

Although there is no single way of identifying whether a child is likely to be susceptible to an extremist ideology, there are possible indicators that should be taken into consideration alongside other factors and contexts. Background factors combined with specific influences such as family and friends may contribute to a child's vulnerability. Similarly, radicalisation can occur through many different methods (such as social media or the internet) and settings (such as within the home).

The Prevent duty

All schools and colleges are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015 (the CTSA 2015), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty.

The Prevent duty should be seen as part of schools' and colleges' wider safeguarding obligations. Designated safeguarding leads and other senior leaders in schools should familiarise themselves with the revised Prevent duty guidance: for England and Wales, especially paragraphs 57-76, which are specifically concerned with schools (and also covers childcare). Designated safeguarding leads and other senior leaders in colleges should familiar themselves with the Prevent duty guidance: for further education institutions in England and Wales. The guidance is set out in terms of four general themes: risk assessment, working in partnership, staff training, and IT policies.

Online Safety within 'Keeping Children Safe in Education' 2023

Additional support

London Grid for Learning have also produced useful resources on Prevent (Online Safety Resource Centre - London Grid for Learning (lgfl.net).

Practice Implications

- This section highlights the role of the internet as a tool for radicalisation and in the potential accidental and deliberate exposure to extremist views and content online. It also identifies responsibilities for childcare and schools to have IT policies in place and should be approached as part of implementing 'appropriate filtering and monitoring' as identified within part two.
    - The 'Educate Against Hate' site is designed to equip school and college leaders, teachers and parents with the information, tools and resources they need to recognise and address extremism and radicalisation in young people, and this includes online issues.
    - Further information for Kent schools (including contact information for the Prevent Education Officers, local procedures, tools and training) can be found on Kelsi .

Sexual violence and sexual harassment between children in schools and colleges

Sexual violence and sexual harassment can occur between two children of any age and sex from primary to secondary stage and into colleges. It can also occur online. It can also occur through a group of children sexually assaulting or sexually harassing a single child or group of children.

Children who are victims of sexual violence and sexual harassment will likely find the experience stressful and distressing. This will, in all likelihood, adversely affect their educational attainment and will be exacerbated if the alleged perpetrator(s) attends the same school or college. Sexual violence and sexual harassment exist on a continuum and may overlap, they can occur online and face to face (both physically and verbally) and are never acceptable.

It is essential that all victims are reassured that they are being taken seriously and that they will be supported and kept safe. A victim should never be given the impression that they are creating a problem by reporting sexual violence or sexual harassment. Nor should a victim ever be made to feel ashamed for making a report. Detailed advice is available in Part five of this guidance.

Additional advice and support

This section includes links to many online safety resources and organisations which can support school/college safeguarding practice. We recommend schools/colleges use these organisations as a starting point for their online safety approaches.

Action points:

- Are DSLs aware of the guidance within annex B and the associated national resources and local support available?
- How does the DSL ensure and evidence that annex B has been read and understood by all school/college leaders, and all staff who work directly with children?
- Do your schools/college policies and procedures reflect the specific safeguarding risks identified within annex B?

Online Safety within 'Keeping Children Safe in Education' 2023

Annex C: Role of the designated safeguarding lead

Practice Implications

- This section highlights the roles and responsibilities of the DSL(s) including managing referrals, working with others, training, record keeping, awareness raising and availability; this will also apply to online safety concerns. DSLs should raise awareness of recognising, responding, recording and referring online safeguarding issues in line with their school/college child protection policies and procedures with all members of staff.
- Whilst the activities of the designated safeguarding lead can be delegated to appropriately trained deputies (trained to the same level as the DSL), the ultimate lead responsibility for child protection, remains with the DSL and this lead responsibility should not be delegated.
- During term time, the DSL (or a deputy) should always be available (during school or college hours for staff to discuss any safeguarding concerns; this will include responding to online safety concerns. It is a matter for individual schools and colleges, working with the DSLs, to define what "available" means and whether in exceptional circumstances availability via phone or other such media is acceptable and to arrange adequate and appropriate cover arrangements for any out of hours/out of term activities.

Online safety is explicitly mentioned in the following contexts:

Governing bodies and proprietors should ensure an appropriate **senior member** of staff, from the school or college **leadership team**, is appointed to the role of designated safeguarding lead. The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place). This should be explicit in the role holder's job description.

Practice Implications

- This section has been updated to add a reference to the DSLs responsibility for filtering and monitoring processes.

Working with others

The designated safeguarding lead is expected to…

- act as a source of support, advice and expertise for all staff…
- liaise with staff (especially teachers, pastoral support staff, school nurses, IT technicians, senior mental health leads and special educational needs coordinators (SENCO's), or the named person with oversight for SEND in a college and senior mental health leads) on matters of safety and safeguarding and welfare (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies so that children's needs are considered holistically…

Practice Implications

- This recognises that DSLs will need to liaise with other staff who may have knowledge or expertise related to online and digital safety.

Online Safety within 'Keeping Children Safe in Education' 2023

Action points:

- How does the DSL (and any deputies) work with other appropriate staff, as required with regards to dealing with online safety concern or making policy decisions?
    - How is this evidenced?

Raising awareness

The designated safeguarding lead should:

- ensure each member of staff has access to, and understands, the school's or college's child protection policy and procedures, especially new and part-time staff
- ensure the school's or college's child protection policy is reviewed annually (as a minimum) and the procedures and implementation are updated and reviewed regularly, and work with governing bodies or proprietors regarding this
- ensure the child protection policy is available publicly and parents know that referrals about suspected abuse or neglect may be made and the role of the school or college in this
- link with the safeguarding partner arrangements to make sure staff are aware of any training opportunities and the latest local policies on local safeguarding arrangements…

Practice Implications

- This will include raising awareness of online safety, developing local knowledge of support available, and ensuring online safety is addressed appropriately within the school/college policies.

Training, knowledge and skills

The designated safeguarding lead (and any deputies) should undergo training to provide them with the knowledge and skills required to carry out the role….Training should provide designated safeguarding leads with a good understanding of their own role, how to identify, understand and respond to specific needs that can increase the vulnerability of children, as well as specific harms that can put children at risk, and the processes, procedures and responsibilities of other agencies, particularly children's social care, so they:

- are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college
- can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online

In addition to the formal training set out above, their knowledge and skills should be refreshed (this might be via e-bulletins, meeting other designated safeguarding leads, or simply taking time to read and digest safeguarding developments) at regular intervals, as required, and at least annually, to allow them to understand and keep up with any developments relevant to their role.

Online Safety within 'Keeping Children Safe in Education' 2023

Practice Implications

- DSLs should access appropriate national and local online safety support and training to ensure they understand online safety risks which could affect their community.
- DSLs should be able to evidence they take appropriate steps to ensure that their settings online safety practice is in line with national and local guidance and procedures.
- Information about online safety is available for Kent DSLs through the Education Safeguarding Service Child Protection Newsletter, Kent Online Safety Twitter feed and the Education People Blog.
- Kent DSLs can also access specific online safety consultations and online safety training via the Education Safeguarding Service.

Action points:

- Has the DSL (and any deputies) accessed appropriate training and support regarding online safety? How is this evidenced?
- Do DSLs:
  - develop an up-to-date awareness of both the risks and benefits of technology?
  - Have an awareness of national and local policy and procedures?
  - understand issues relating to online safety and SEND?

Understanding the views of children

It is important that all children feel heard and understood. Therefore, designated safeguarding leads (and deputies) should be supported in developing knowledge and skills to:

- encourage a culture of listening to children and taking account of their wishes and feelings, among all staff, and in any measures the school or college may put in place to protect them, and
- understand the difficulties that children may have in approaching staff about their circumstances and consider how to build trusted relationships which facilitate communication

Practice Implications

- This will include online safety.

Action points:

- How does your school/college evidence that you listen to children relating to their online lives?