Online Safety within 'Keeping Children Safe in Education' 2021

On the 6th July 2021 the Department for Education (DfE) published the updated 'Keeping children safe in education' (KCSIE) guidance ready for implementation from the 1st September 2021. Schools and Colleges must comply with KCSIE 2020 until that date.

KCSIE is statutory guidance and all schools and colleges must have regard to it when carrying out their safeguarding. 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.

This document only focuses on elements of KCSIE 2021 relevant to **online safety**. Designated Safeguarding Leads (DSLs) and leaders should read the entire document when evaluating their wider safeguarding practice.

Summary of key online safety requirements and changes within KCSIE 2021

- Specific online safety content has been added and strengthened to ensure online safety is clearly viewed as part of a school and college's statutory safeguarding responsibilities.
- The DSL continues to have overall responsibility for online safety; they can be supported by appropriately trained deputies and should liaise with other staff as appropriate, but this responsibility cannot be delegated.
- DSLs should continue to 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.
- Online safety content relating to staff training and teaching children about safeguarding has been updated: All staff should continue to be provided with online safety information and training at induction, and the importance of receiving online safety training as part of regular (at least annual) child protection training and updates has been empathised. Children should be taught about online safety, including as part of statutory Relationships and Sex Education (RSE), but 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.
- Additional content and guidance relating to peer on peer abuse has been added throughout and part five continues to recognise that child on child sexual violence and sexual harassment can occur online.
- Schools and colleges should ensure their child protection policy and wider safeguarding policies specifically address online safety, especially with regards to online peer on peer abuse, relationships on social media and the use of mobile and smart technology.
- KCSIE 2021 now references four areas of risk online within part two: content, contact, conduct and commerce. 2020 referred to content, contact and conduct.
- Additional content has been included in annex B with regards to cybercrime and the safeguarding implications.
- Annex D contains updated links to online safety resources to support schools and colleges.

What this means for DSLs and leaders

- Online safety should be considered to be part of your statutory safeguarding responsibilities and requires a whole-school/college approach.
- Ensure your policies, education approaches and staff training address the breadth of online safety issues as identified in KCSIE 2021; 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 online peer on peer abuse including cyberbullying, and the use of mobile and smart technology.
- 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 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.
- Ensure all staff are aware of the policies and procedures to follow with regards to responding to online safety concerns, including online peer on peer abuse issues.
- Ensure the 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.
- DSLs from all school and college types should ensure they have accessed the UKCIS 'Sharing nudes and semi-nudes: advice for education settings working with children and young people' guidance and are familiar with its content and when it should be followed.
- Ensure appropriate filtering and monitoring approaches are in place which are suitable for the local context and use of technology.
- Remote learning should be implemented in a safe and secure way.
- There should be regular and appropriate parental engagement in online safety, however specific concerns should be responded to in line with child protection policies.
- Online safety approaches should be regularly reviewed and updated as required.

How to read this document

- This font indicates a direct quote from the KCSIE 2021 guidance.
- This font indicates online safety specific content.
- This font is used to highlight recommendations, best practice and useful links.
- This font indicates a possible action points for DSLs and school/college leaders to consider in readiness for September 2021.

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:

- behaviour policy (which should include measures to prevent bullying, including cyberbullying, prejudice-based and discriminatory bullying) …

14. All staff should receive appropriate safeguarding and child protection training (including online safety) 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 provide them with relevant skills and knowledge to safeguard children effectively.

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 online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic 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).

- 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.
- Online safety concerns should be reported to the DSL or a deputy.

Action points

- Does your child protection policy make is clear that 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)

- This specifically identifies that cyberbullying can be considered as emotional abuse.

- Anti-bullying policies should be up-to-date and include the settings 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

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 … 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 (also known as peer on peer abuse) in education and all staff should be aware of it and of their school or colleges policy and procedures for dealing with it.

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

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 as drug taking and or alcohol misuse, deliberately missing education and consensual and non-consensual sharing of nude and semi-nude images and/or videos can be signs that children are at risk. Other safeguarding issues all staff should be aware of include….

- 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.

Child Sexual Exploitation (CSE)

36. 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 e.g. through others sharing videos or images of them on social media.

- 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

Peer on peer abuse (child on child)

46. All staff should be aware that children can abuse other children (often referred to as peer on peer abuse). And that it can happen both inside and outside of school or college and online. It is important that all staff recognise the indicators and signs of peer on peer abuse and know how to identify it and respond to reports.

47. 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 peer on peer abuse, they should speak to their designated safeguarding lead (or deputy).

    - This is especially likely to be the case where there is online peer on peer 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.

48. It is essential that all staff understand the importance of challenging inappropriate behaviours between peers, many of which are listed below, that are actually 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.

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

49. Peer on peer 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 peers
    - 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); For further information about sexual violence see Annex B.
    - 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 nudes 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
    - 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).

- The updates for 2021 clearly identify that technology can play a key role within peer on peer abuse concerns. Therefore it is essential schools and colleges reflect this within any peer on peer abuse policies, procedures and approaches.

49. All staff should be clear as to the school's or college's policy and procedures with regards to peer on peer 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.

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

Action points

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

Part two: The management of safeguarding

Safeguarding policies and procedures

84. 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.

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

- an effective child protection policy which:
  - reflects the whole school/college approach to peer on peer abuse
  - includes policies as reflected elsewhere in Part two of this guidance, such as online safety,
  - should be 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
  - is available publicly either via the school or college website or by other means.

- Individual schools and colleges should have a specific and robust child protection policy which is updated at least annually and is publicly available.
- It is not a statutory requirement to have a separate online safety policy, however schools and colleges should ensure key online elements (such as peer on peer abuse, filtering and monitoring, social media and use of mobile technology) are addressed within their child protection policy or other relevant safeguarding policies.
- 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)

- 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.

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

86. 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.

- All members of staff should to be provided with information about acceptable use of technologies, staff/pupil relationships and the use of social media as part of induction.

Action points:

- Does your child protection policy include online safety or do you have a standalone online safety policy?
    - Is it up to date?
    - Is it publicly available and do all members of the community know how to access it?
- 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?
    - 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?

The designated safeguarding lead

89. 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). This should be explicit in the role-holder's job description (see Annex C, which describes the broad areas of responsibility and activities related to the role).

91. Whilst the activities of the designated safeguarding lead can be delegated to appropriately trained deputies, the ultimate lead responsibility for safeguarding and child protection, as set out above, remains with the designated safeguarding lead. This responsibility should not be delegated.

95. In addition to their formal training …. their knowledge and skills should be updated (for example via e-bulletins, meeting other designated safeguarding leads, or taking time to read and digest safeguarding developments), at regular intervals, and at least annually, to keep up with any developments relevant to their role.

- 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, the overall responsibility for online safety is explicitly held by the Designated Safeguarding Lead (DSL) and this 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.
- DSLs should consider how they evidence their knowledge and skills regarding online safety are updated at regular intervals.

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?
- How does your DSL keep their knowledge and skills in relation to online safety updated? How is this evidenced?

Information sharing

Paragraphs 105-113 explore responsibilities with regarding to information sharing, including transfer or records.

- Schools and colleges responsibilities apply to the storage and sharing of information held and kept within electronic as well as paper recording systems.
- 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.

113. In addition to the child protection file, the designated safeguarding lead should also consider if it would be appropriate to share any information with the new school or college in advance of a child leaving….More information on the child protection file is in Annex C.

- This should include if there have been any online safety concerns.

Staff training

114. Governing bodies and proprietors should ensure that all staff undergo safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. Induction and training should be in line with any advice from the safeguarding partners.

115. 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.

116. 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

117. 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.

- 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.
    - Settings should consider how this is implemented, for example, will it 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 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.
- 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 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 e.g. via email, e-bulletins and staff meetings?
- How do you evidence all of this is in place?

Opportunities to teach safeguarding

119. Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety, and recognise that a one size fits all approach may not be appropriate for all children, and a more personalised or contextualised approach for more vulnerable children, victims of abuse and some SEND children might be needed.

120. Schools should consider all of this as part of providing a broad and balanced curriculum (colleges may cover relevant issues through tutorials). This may include covering relevant issues for schools through Relationships Education (for all primary pupils) and Relationships and Sex Education (for all secondary pupils) and Health Education (for all pupils in state-funded schools). The statutory guidance can be found here: Statutory guidance: relationships education relationships and sex education (RSE) and health education.

- Paragraph 121 signposted to specific resources which could support online safety education.

- Governing bodies and proprietors should ensure that online safety is specifically covered within their safeguarding 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 e.g. 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.
    - 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.
- Settings 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.
- One-off events, lessons or assemblies or a reliance on external speakers, are not effective or adequate practice.
    - 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/colleges 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 appropriate staff within your school/college familiar with the resources identified in paragraphs 121?
- 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?

122. 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.

- 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

- This section has been significantly updated for 2021; it includes new content and integrates content previously covered in annex C 'Online Safety' of KCSIE 2020. This change emphasises the importance of online safety being recognised as part of school and colleges statutory safeguarding responsibilities.

123. 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.

- This clearly identifies online safety as a safeguarding responsibility and highlights the need for settings to ensure that all members of their communities can develop appropriate understanding and skills to prepare them to respond to online safety issues.

124. 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/)

- This section has been updated to include a fourth area of risk – 'Commerce'.
- 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.
- The advice given by the school or college should empower their community to be able to respond to a range of online threats 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.

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?

125. Schools and colleges should ensure online safety is a running and interrelated theme whilst devising and implementing 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 any parental engagement.

- The section clearly identifies that online safety requires an embedded a long term whole school/college approach and should not be viewed as a one-off 'tick box' input or event.
- 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 e.g. 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 e.g. 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.

Online safety policy

126. Online safety and the school or college's approach to it should be reflected in the child protection policy. Considering the 4Cs 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. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass their peers 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 in their mobile and smart technology policy and their child protection policy.

- Online safety should be clearly referenced as part of the school/college child protection policy.
- Schools and colleges should have a clear policy regarding the schools/colleges decisions with regards to the use of mobile and smart technology e.g. wearable technology. The policy should specifically address how person use of mobile and smart technology will be managed on site.
- The Education Safeguarding Service provide a template mobile technology policy which schools and colleges can adapt.

Action points:

- Does the setting have a clear policy regarding use of mobile technology, including phones and other personal devices?
    - How is this communicated to staff, learners and parents/carers?

Remote learning

127. Where children are being asked to learn online at home the Department has provided advice to support schools and colleges do so safely...

- Paragraph 127 provides links to specific remote learning guidance from the DFE, NSPCC and PSHE associate guidance.
- 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.

Filters and monitoring

128. Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place. Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs vs risks.

129. The appropriateness of any filters 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. The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like.

- Paragraph 130 details support and guidance for schools regarding buying and procurement.

- 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.
- Governing bodies and proprietors should ensure that the welfare of children and young people is paramount and that any decisions taken regarding filtering and monitoring systems are taken from a safeguarding, educational and technical approach. These 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 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, governing bodies and proprietors 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 and 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.
    - SWGfL also have a 'Test Filtering' tool which allows schools and colleges to check their Internet Service Providers filtering approaches.

- 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 include appropriate supervision, implementing an Acceptable Use Policy (AUP), a robust and embedded online safety curriculum and staff training etc.

Action points:

- Has the leadership accessed the UK Safer Internet centre (and any local guidance) material regarding appropriate filtering and monitoring?
- Does the leadership team understand the current filtering/monitoring systems in place?
    - 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 evidenced?
- How is this information shared with the community? For example, is filtering and monitoring explicitly covered within the child protection policy?
- How do SLT work with the technical team (e.g. broadband provider, IT Technicians, Network Managers or IT service providers) to make filtering and monitoring decisions and take action on concerns identified?
    - If so, how is this documented?
- 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 e.g. 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

131. 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, broader guidance on cyber security including considerations for governors and trustees can be found at NCSC.GOV.UK.

- School and college leaders should work with their DSLs and technical staff/support to ensure appropriate security protection procedures are in place which will safeguard their systems and community.
- The specific approaches require will vary but is 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:

- 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?

Reviewing online safety

132. 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.

133. 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.

134. 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.

Action points:

- How do you evidence that your school/college is reviewing your online safety practice regularly and making changes as required?

Information and support

135. 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 D.

- The updated guidance in annex D links to a range of updated sources of support and resources.
    - The Education Safeguarding Adviser (Online Protection) and the Online Safety Development Officer are located within the Education Safeguarding Service and provide educational settings in Kent with targeted online safety advice, guidance and training.
    - Local information about online safety is provided for DSLs through the Education Safeguarding Service Child Protection Newsletter, Kent Online Safety Twitter feed and the Education People Blog.

Action points:

- How does the setting (especially the DSL) evidence that they are keeping up to date with developments within the online safety agenda?

Peer on peer /child on child abuse

144. All staff should recognise that children are capable of abusing their peers (including online). All staff should be clear about their school's or college's policy and procedures with regard to peer on peer abuse.
145. Governing bodies and proprietors should ensure that their child protection policy includes:

- procedures to minimise the risk of peer on peer 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 peer on peer abuse will be recorded, investigated and dealt with
- clear processes as to how victims, perpetrators and any other children affected by peer on peer abuse will be supported
- a recognition that even if there are no reported cases of peer on peer 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 peer on peer abuse is unacceptable and will be taken seriously
- the different forms peer on peer abuse can take, such as:
    - bullying (including cyberbullying, prejudice-based and discriminatory bullying)
    - abuse in intimate personal relationships between peers
    - 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 and Sexual violence and sexual harassment between children in schools and colleges sets out how schools and colleges should respond to reports of sexual violence and sexual harassment
    - Consensual and non-consensual sharing of nudes 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 nudes and semi-nudes 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
    - initiation/hazing type violence and rituals.

- 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 are capable of abusing their peers online? How do you know this is achieved?
- Does your child protection policy clearly identify policies and procedures to follow when responding to online peer on peer abuse concerns e.g. consensual and non-consensual sharing of nudes and semi-nude images and/or videos?

Part five: Child on child sexual violence and sexual harassment

428. This part of the statutory guidance is about how schools and colleges should respond to all 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).

429. Sexual violence and sexual harassment can occur between two children of any age and sex, from primary through to secondary stage and into colleges. It can occur 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. 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'.

- DSLs should read part five alongside the updated 'Sexual Violence and Sexual Harassment Between Children in Schools and Colleges' guidance.
- Childnet's project deSHAME provides useful information for educational settings regarding online sexual violence and harassment.

The immediate response to a report: Responding to the report

444. 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…

- where the report includes an online element, 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.

- 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 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
  - 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 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.
  - children and young people under the age of 18 sharing adult pornography or exchanging sexual texts which do not contain images. Schools and colleges should respond to these peer on peer abuse concerns in line with existing policies, for example their child protection, mobile technology and behaviour policies.
- Schools 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?

Action following a report of sexual violence and/or sexual harassment: What to consider

448. 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.

Ongoing response: Safeguarding and supporting the victim

456. The following principles are based on effective safeguarding practice and should help shape any decisions regarding safeguarding and supporting the victim.

- Paragraph 456 links to specific tools which can be used when online abuse is a concern including Childline and the Internet Watch Foundation (IWF)
  - Report Remove is a free tool from Childline and the IWF which 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.

Annex B: Further information

- 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 forms of abuse listed in annex B specifically include references to technology and/or online behaviour or risks

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.

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.

- This is a new section which has been added within safeguarding priorities. Whilst it is likely some education will be delivered by 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 and colleges child protection and safeguarding policies and procedures.

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

- 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 e.g. Kent Police.

Domestic abuse

- The domestic abuse content has been updated to reflect that 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 definition of domestic abuse now captures a range of different abusive behaviours, including physical, emotional and economic abuse and coercive and controlling behaviour which may take place online, for example 'cyberstalking'. 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 gender, age, ethnicity, socioeconomic status, sexuality or background and domestic abuse can take place inside or outside of the home.
- Although aimed at safeguarding individuals over 18 and not covered within KCISE 2021, 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 is 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.

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…

There is no single way of identifying whether a child is likely to be susceptible to an extremist ideology. 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). However, it is possible to protect vulnerable people from extremist ideology and intervene to prevent those at risk of radicalisation being radicalised.

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.

- 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 procedures, tools and training) can be found on Kelsi .

Sexual violence and sexual harassment between children in schools and colleges

- This content has been significantly updated and a number of additional resources, toolkits and supporting documents, specific to online issues are highlighted. Key online specific elements include:

Sexual harassment

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.

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

- 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 nudes and semi-nudes images and/or videos. As set out in UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people (which provides detailed advice for schools and colleges) taking and sharing nude photographs of U18s is a criminal offence
    - sharing of unwanted explicit content
    - upskirting (is a criminal offence)
    - sexualised online bullying
    - unwanted sexual comments and messages, including, on social media
    - sexual exploitation; coercion and threats

Upskirting

The Voyeurism (Offences) Act 2019, which is commonly known as the Upskirting Act, came into force on 12 April 2019. 'Upskirting' is where someone takes a picture under a persons clothing (not necessarily a skirt) without their permission and or knowledge, with the intention of viewing their genitals or buttocks (with or without underwear) to obtain sexual gratification, or cause the victim humiliation, distress or alarm. It is a criminal offence. Anyone of any sex, can be a victim.

Action points:

- Are DSLs aware of the new and updated terms within Annex B and the associated resources and local support available?
- Have DSLs ensured that staff who work directly with children and young people have read and understood annex B? How do you evidence this?

- Do your schools/college policies and procedures reflect the risks identified within Anne B?

Annex C: Role of the designated safeguarding lead

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 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. 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). This should be explicit in the role holder's job description.

Working with others

The designated safeguarding lead is expected to… liaise with staff (especially teachers, pastoral support staff, school nurses, IT Technicians, senior mental health leads and special educational needs coordinators (SENCOs), or the named person with oversight for SEN 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.

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?

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.

- DSLs should access appropriate 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.

- In Kent, specific training for DSL is available via Kent CPD online.
- Information about online safety is provided for Kent DSLs through the Education Safeguarding Service Child Protection Newsletter, Kent Online Safety Twitter feed and the Education People Blog. Kent DSLs can access specific online safety consultations via the Education Safeguarding Service.

Action points:

- Has the DSL accessed appropriate training and support regarding online safety?
  - Does this include:
    - developing an up-to-date awareness of both the risks and benefits of technology?
    - an awareness of national and local policy and procedures?
    - An exploration of issues relating to online safety and SEND?
  - How is this evidenced?

Annex D – Online Safety

This section highlights some of the information available to support schools, colleges and parents/carers to keep children safe online. Annex D is not an exhaustive list but should provide a useful starting point.

Summary

Since the widescale use of technology as a tool for learning, socialising and play as a result of the Covid-19 pandemic, online safety must continue to be recognised by schools and colleges as a key safeguarding consideration. The inclusion of online safety within part two strengthens the approaches that DSLs and schools and college leaders are required to implement to ensure they are able to protect their communities online.

The online safety agenda continue to evolve and increase; it is therefore essential that DSLs, governing bodies and proprietors evidence the recognition of online safety within their statutory safeguarding responsibilities and implement approaches which will safeguard their community online.

DSLs and leaders in schools and colleges should review their current online safety practice and implement any changes as required from 1st September 2021.

Online Safety Support 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.

Our Safeguarding Support Package for Schools is available to schools and colleges in Kent and beyond and contains a number of online safety resources including template staff training resources, a specific online safety policy and a targeted webinar for DSLs.

The Education Safeguarding Service provide a number of training courses and services 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.