‘Keeping Children Safe in Education’ 2020: Online Safety Content and Updates

On the 17th June 2020 the Department for Education (DfE) published the updated ‘Keeping children safe in education’ (KCSIE) guidance ready for implementation from the 1st September 2020. Schools and Colleges must comply with KCSIE 2019 until that date. KCSIE is statutory guidance from the DfE; all schools and colleges must have regard to it when carrying out their duties to safeguard and promote the welfare of children.

This document only focuses on elements of KCSIE 2020 relevant to **online safety**. It is recommended that DSLs and leaders read the entire KCSIE 2020 document when evaluating their wider safeguarding practice.

Summary of key online safety requirements and changes within KCSIE 2020:

- DSLs continue to have overall responsibility for online safety (Annex B) and this cannot be delegated. They can be supported by appropriately trained deputies and liaise with other staff on matters of online safety.
- DSLs should continue to be able 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.
- All staff should continue to be provided with online safety training at induction and as part of regular child protection training and updates.
- Part 5 continues to recognise that child on child sexual violence and sexual harassment can occur on and offline.
- Additions have been made to content relating to Child Sexual Exploitation and Child Criminal Exploitation to recognise the role technology can play.
- An additional section has been added to part one to help staff make the link between mental health concerns and safeguarding issues. Whilst online safety is not specifically addressed, the section signposts to guidance and resources where online safety is explored.
- Links to additional or updated resources have been included to support schools and colleges in teaching online safety to all learners as part of providing a broad and balanced curriculum, including as part of the requirements for Relationships Education and Relationships and Sex Education.
- Additional information is available on how to support keeping children safe online when they are learning at home within annex C.
- Content relating to ‘Upskirting’ has been updated to reflect that anyone of any gender, can be a victim.
- Additional links to new guidance and resources related to online safety have been added throughout and particularly in annex C.

How to read this document:

- This font indicates a direct quote from the KCSIE 2020 guidance.
- This font indicates content has been added or amended from KCSIE 2019.
- This font is used to highlight recommendations, best practice and useful links.
- This font indicates a possible action points for DSLs and senior leadership staff to consider in readiness for September 2020.

Note: 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.

Governing bodies, proprietors, academy trusts **must** ensure that all staff read at least part one of the guidance. They should also ensure that mechanisms are in place to assist staff to understand and discharge their role and responsibilities as set out in part one of the guidance.

Part one: Safeguarding information for all staff

What school and college staff should know and do

2. Safeguarding and promoting the welfare of children is **everyone's** responsibility. **Everyone** who comes into contact with children and their families has a role to play. In order to fulfil this responsibility effectively, all practitioners should make sure their approach is child-centred. This means that they should consider, at all times, what is in the **best interests** of the child.
    - Safeguarding is identified as a responsibility for all members of educational settings communities. It should be made clear to all staff, children and parents that this applies to any concerns and behaviours taking place online as well as offline.
    - When responding to online concerns, the best interests of the child should always be considered.

What school and college staff should look out for

21. **All** staff should be aware that safeguarding incidents and/or behaviours can be associated with factors outside the school or college and/or can occur between children outside of these environments. **All** staff, but especially the designated safeguarding lead (and deputies) should consider whether children are at risk of abuse or exploitation in situations outside their families. Extra-familial harms take a variety of different forms and children can be vulnerable to multiple harms including (but not limited to) sexual exploitation, criminal exploitation, and serious youth violence.
    - This statement has been updated.
    - All staff should recognise that online safety issues that occur offsite should be considered in the same way as other offsite safeguarding concerns.

Indicators of abuse and neglect

24**. 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 emotionally abusive. 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 cyberbullying?

- Does your policy outline the procedures for children, staff and parents to follow if cyberbullying concerns are reported?

25. **Sexual abuse**: …may 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…
    - This specifically identifies that sexual abuse can occur via the internet and can involve a range of online behaviours.

Action points

- Does your child protection policy clearly identify the use of technology as a potential risk to members of the community?

27. All staff **should** have an awareness of safeguarding issues that can put children at risk of harm. Behaviours linked to issues such as…sexting (also known as youth produced sexual imagery) put children in danger.
    - This specifically identifies that staff should have an awareness of sexting.

Action points

- How can you evidence that your staff have an awareness of 'sexting'?

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

28. Both CSE and CCE are forms of abuse and both occur where an individual or group takes advantage of an imbalance in power to coerce, manipulate or deceive a child into sexual or criminal activity. …. Victims can be exploited even when activity appears consensual and it should be noted exploitation as well as being physical can be facilitated and/or take place online. More information include definitions and indicators are included in Annex A.
    - New content. This paragraph explicitly identifies that CSE and CCE can take place online.

29. All staff should be aware that safeguarding issues can manifest themselves via peer on peer abuse. This is most likely to include, but may not be limited to:
    - bullying (including cyberbullying); ….
    - sexual harassment, such as sexual comments, remarks, jokes and online sexual harassment, which may be stand-alone or part of a broader pattern of abuse,
    - Upskirting which typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm;
    - sexting (also known as youth produced sexual imagery) …
    - All members of staff should be aware of range of safeguarding issues; this specifically includes staff being aware of cyberbullying, online sexual harassment, 'upskirting' and sexting.

30. **All** staff should be clear as to the school or college's policy and procedures with regards to peer on peer abuse.
    - This will include online peer on peer abuse.

Action points

- Does your child protection policy clearly identify peer on peer abuse issues involving technology, such as cyberbullying, upskirting and sexting?
- Do you provide enough training to members of staff regarding peer on peer abuse, including cyberbullying, upskirting and sexting?
- Do you provide appropriate training and information to members of staff regarding identifying online contextual safeguarding issues?

Mental Health

- New section added.

34. All staff should also be aware that mental health problems can, in some cases, be an indicator that a child has suffered or is at risk of suffering abuse, neglect or exploitation.

35. Only appropriately trained professionals should attempt to make a diagnosis of a mental health problem. Staff however, are well placed to observe children day-to-day and identify those whose behaviour suggests that they may be experiencing a mental health problem or be at risk of developing one.

36. 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 and education.
    - Mental health problems could indicate that a child may have suffered or is at risk of suffering online abuse, neglect or exploitation.
    - Staff may observe online behaviours which indicate a child has experienced abuse or neglect or may be experiencing a mental health problem or be at risk of developing one.
    - Mental health issues can manifest through online behaviours; this behaviour could be overt (for example children deliberately accessing or sharing pro self-harm or pro-eating disorder forums and/or content) or could be more subtle.
    - Staff should be encouraged to consider mental health concerns as possible underlying factors when addressing online behaviours or online behaviour changes.

38. The department has published advice and guidance on Preventing and Tackling Bullying, and Mental Health and Behaviour in Schools (which may also be useful for colleges). In addition, Public Health England has produced a range of resources to support secondary school teachers to promote positive health, wellbeing and resilience among young people including its guidance Promoting children and young people's emotional health and wellbeing. Its resources include social media, forming positive relationships, smoking and alcohol. See Rise Above for links to all materials and lesson plans.
    - Paragraph 38 links to guidance and curriculum resources which address and include online safety.

Action points

- Do your staff recognise that mental health concerns could indicate online abuse?
- Are staff aware that mental health concerns may present through online behaviours?

Part two: The management of safeguarding

Safeguarding policies

62. 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.

63. This should include:
    - Individual schools and colleges having an effective child protection policy…It should be updated annually (as a minimum) and be 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 setting should ensure key elements (such as filtering and monitoring, social media and use of mobile technology) are addressed within the 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 staff behaviour policy (sometimes called the code of conduct) which should, amongst other things, include acceptable use of technologies, 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. They should be reviewed at least annually and shared with staff on a regular basis.
        - The Education People provide a template Acceptable Use Policy (AUP) and online safety policy template which can be used by to develop and support a staff behaviour policy.

64. ... These policies and procedures, along with Part one of this guidance and information regarding the role and identity of the designated safeguarding lead (and any 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 issues in relation to online safety, either within the child protection policy or as a separate policy?
    - Is it up to date?
    - Is it publicly available - do all members of the community know how to access it?
- 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

67. 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…

68. …. Any deputies should be trained to the same standard as the designated safeguarding lead.

69. Whilst the activities of the designated safeguarding lead can be delegated to appropriately trained deputies, the ultimate **lead responsibility** for safeguarding and child protection…remains with the designated safeguarding lead. This responsibility should not be delegated.
    - The ultimate responsibility for online safety falls within the remit of the Designated Safeguarding Lead (DSL).
        - Staff with appropriate skills, interest and expertise regarding online safety (such as computing leads or technical staff) should be encouraged to help support the DSL as appropriate, for example when developing curriculum approaches or making technical decisions. However, settings should be clear that overall responsibility for online safety cannot be delegated and remains with the DSL.

Action points:
- Is the settings DSL the lead person responsible for online safety?
    - Is this made clear to all members of staff?
    - How does the setting evidence that the DSL has lead responsibility?
- Has the school 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?

70. … NPCC- When to call the police should help designated safeguarding leads understand when they should consider calling the police and what to expect when they do.
    - Link to new NPCC guidance has been added. DSLS should read this guidance to support decision making regarding police involvement in all safeguarding concerns, including online safety issues.

Information sharing

Paragraphs 82-88 explore responsibilities with regarding to information sharing, including transfer or records. Paragraph 84 was updated to provide further clarification about GDPR and withholding information. Paragraph 86 was updated to include a link to the data protection toolkit.
- 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.

Staff training

89. 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 advice from the local three safeguarding partners.
    - Child protection training should explicitly cover online safety as part of all staff members induction.

90. In addition, all staff should receive regular safeguarding and child protection updates (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.
    - Settings should consider how online safety is covered within annual safeguarding updates provided to staff; settings may decide to integrate online safety within current child protection training or provide separate sessions.
        - Local good practice examples identified include covering safeguarding (including online safety) as a standing item at staff meetings and providing specific online safety trainings sessions as part of an annual training calendar of events.

Action points:

- Is online safety covered explicitly within your induction process for new staff?
- How does your setting provide appropriate, up-to-date and relevant whole staff online safety training?
- How does your setting involve staff in developing and contributing to online safety policies and procedures?

Online safety

92. As schools and colleges increasingly work online, it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such, governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place. Additional information to support governing bodies and proprietors keep their children safe online (including when they are online at home) is provided in Annex C
    - This paragraph has been updated to make clear that additional information is available in Annex C on how to support keeping children safe online when they are learning at home.
    - Online safety is clearly viewed as part of settings safeguarding responsibilities settings should recognise the role of the internet within child protection concerns and ensure appropriate systems are in place to filter and monitor internet activity.
        - The UKCIS Education Group has developed guidance for school governors to help governing boards support their DSL to keep children safe online.

Action points:

- Does your setting clearly view online safety as a safeguarding issue?
    - How do you evidence this?
- Have your DSL, SLT, governing body/proprietor etc. read and understood annex C?
- Have your governors accessed the UKCIS guidance for school governors?
    - Can this be used to help provide evidence of strategic oversight?

Opportunities to teach safeguarding

93. Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety. Schools should consider this as part of providing a broad and balanced curriculum.

94. 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) which will be compulsory from September 2020. Schools have flexibility to decide how they discharge their duties effectively within the first year of compulsory teaching and are encouraged to take a phased approach (if needed) when introducing these subjects. The statutory guidance can be found here: Statutory guidance: relationships education relationships and sex

education (RSE) and health education. Colleges may cover relevant issues through tutorials. The following resources may help schools and colleges:

- DfE advice for schools: teaching online safety in schools
- UK Council for Internet Safety (UKCIS) guidance: Education for a connected world
- National Crime Agency's CEOP education programme: Thinkuknow
- Public Health England: Rise Above

- This paragraph has been updated to reflect mandatory RSHE from September 2020 (now to be implemented from March 2021 following Coivd-19 restrictions) and added additional links to further online safety advice and guidance, including the DfE 'Teaching online safety in schools' guidance.
- Governing bodies and proprietors should ensure that online safety is specifically covered within the curriculum.
    - The responsibility for teaching children about online safety is not the sole responsibility of the computing curriculum; it should also be explicitly taught within RSHE and be woven throughout the curriculum for all age groups. 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 settings ability to develop internal capacity to respond to concerns. UKCIS have published guidance for educational settings regarding the use of external visitors.
        - The SWGfL have produced Project Evolve which aims to provide education resources in line with the strands identified within Education for a connected world.
    - The online safety curriculum should be flexible, relevant and engage learners' interests, be appropriate to their own needs and abilities and encourage them to develop resilience to online risks.
    - 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 is to gain learner input into the online safety curriculum; this could involve use of learner councils or use of peer education approaches.

Action points:

- Are relevant staff within your setting familiar with the resources identified in paragraph 94?
    - How do you evidence this is the case?
- How does your setting teach children about online safety?
    - Are all children receiving education that is relevant and up to date?
    - Is there a clear scheme of work which identifies relevant and appropriate teaching resources?
    - Is the online safety curriculum differentiated to your learners needs, ages and abilities?
- How does your setting identify and target children who may require more specific educational support 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 academic year and across subject areas?
- How does your setting use external speakers to complement internal education approaches?

95. 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' as

outlined in annex c.

Inspection

Paragraphs 96-98 have been updated to reflect changes to Ofsted guidance.

- Ofsted include online safety throughout their guidance, especially with regards to inspecting safeguarding.

Peer on peer abuse

106. Governing bodies and proprietors **should** ensure that their child protection policy includes:
    - different forms peer on peer abuse can take, such as:
        - sexual violence and sexual harassment….
        - …sexting (also known as 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 UK Council for Internet Safety (UKCIS) Education Group has published advice for schools and colleges on responding to sexting incidents; …
    - DSLs should access and follow the UKCIS sexting guidance for schools and colleges. This guidance should be used by DSL to support them in using their professional judgement when responding to sexting concerns.
        - KSCMP provide local advice: responding to harmful behaviours and underage sexual activity and sexting guidance for professionals.

Action points:

- Does your child protection policy identify policies and procedures with regards to responding to online peer on peer abuse?

Part 5: Child on child sexual violence and sexual harassment

268. Governing bodies and proprietors should be aware that the department has published detailed advice to support schools and colleges. The advice is available here: Sexual violence and sexual harassment between children in schools and colleges and includes, what sexual violence and sexual harassment look like, important context to be aware of, related legal responsibilities for schools and colleges and advice on a whole school or college approach to preventing child on child sexual violence and sexual harassment.
    - The guidance clearly identifies that child on child sexual violence and sexual harassment behaviour can take place both on and offline.
        - Childnet's project deSHAME provides useful information for educational settings regarding online sexual violence and harassment.

274. …where the report includes an online element, being aware of searching screening and confiscation advice (for schools) and UKCIS sexting advice (for schools and colleges). 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.
    - DSLs should access the UKCIS guidance and ensure that all staff are aware of how to respond to potential sexting concerns.

Annex A: Further information

Child Criminal Exploitation (CCE)

CCE does not always involve physical contact; it can also occur through the use of technology.

- New statement added to recognise the role the internet can play in CCE. Examples could include gifts of technology and communication and intimidation over social media.

Child Sexual Exploitation (CSE)

…CSE does not always involve physical contact; it can also occur through the use of technology…. It can include both contact (penetrative and non-penetrative acts) and non-contact sexual activity and may occur without the child or young person's immediate knowledge (e.g. through others copying videos or images they have created and posted on social media).

- Updated statement that recognises the role the internet can play in CSE.

Domestic Abuse

- Although not specifically mentioned, the internet can play a role domestic abuse, such as controlling, coercive or threatening behaviour online.

Preventing radicalisation

- 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.
    - The Kent child protection policy template covers responding to concerns regarding radicalisation. Further information about Prevent Duty and the Kent approach (including procedures, tools and training) can be found on Kelsi .
    - The Department for Education has published advice for settings on the Prevent duty.
    - The Government has also launched a website called 'Educate Against Hate', which 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.

Peer on peer/ child on child abuse

- Children can abuse other children. This is generally referred to as peer on peer abuse and can take many forms. This can include (but is not limited to): abuse within intimate partner relationships; bullying (including cyberbullying); ….
- …Sexual violence and sexual harassment exist on a continuum and may overlap, they can occur online and offline (both physical and verbal) and are never acceptable…
- 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:
        - non-consensual sharing of sexual images and videos;
        - sexualised online bullying;
        - unwanted sexual comments and messages, including, on social media; and
        - sexual exploitation; coercion and threats
        - Upskirting
    - This section specifically highlights the role of technology within peer on peer abuse and provides examples of online sexual harassment.

Upskirting

The Voyeurism (Offences) Act, 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 gender, can be a victim.

- This section has been updated to clarify the legislation and to reflect that anyone of any gender can be a victim of 'upskirting'.

Action points:

- Have staff who work directly with children read annex A?
  - How do you evidence this?
- Does your child protection policy include the use of technology as a tool within specific forms of abuse identified in annex A?
- Have the DSL and all staff had appropriate training?
- How are children educated to be aware of the issues identified in annex A appropriately to their context, including age and ability?

Annex B: 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. Settings should raise awareness of recognising, responding, recording and referring online safeguarding issues in line with the child protection policies and procedures with all members of staff.

Online safety is explicitly mentioned in the following contexts:

The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection (including online safety).

- Work with others
  - The designated safeguarding lead is expected to…liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOS …) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies;
    - The DSL holds lead the ultimate lead responsibility for safeguarding and child protection, including online safety. This lead responsibility cannot be delegated. However, appropriately trained deputies can support this and other staff should be liaised with by the DSL as necessary.

Action points:

- Is the DSL clearly identified in policies and procedures as having overall lead responsibly for online safety within your setting?
- How does the DSL work with other staff, as appropriate with regards to dealing with online safety?
  - How is the evidenced?

- Training:
    - In addition to the formal training …, 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 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 SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online…
    - DSLs should access appropriate online safety support and training to enable them to understand online safety risks. DSLs should be able to evidence they take appropriate steps to ensure that 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 DSLs through the Education Safeguarding Service Child Protection Newsletter, Kent Online Safety Twitter feed and the Education People Blog. Kent DSLs are also able to 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 C: Online safety

The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation – technology often provides the platform that facilitates harm. An effective approach to online safety empowers a school or college to protect and educate the whole school or college community in their use of technology and establishes mechanisms to identify, intervene and escalate any incident 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.

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

- **content**: being exposed to illegal, inappropriate or harmful material; for example, pornography, fake news, racist or radical and extremist views;
- **contact**: being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults; and
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, or online bullying.

- Online safety messages shared with staff and children should be appropriate and up-to-date and reflect the full range of risks; content, contact and conduct. The advice should empower them to be able to respond to a range of online threats as well as opportunities.
- Settings should develop and implement a curriculum that is appropriate to the needs of their learners, that covers a range of online safety issues identified above.

Action points:

- Are staff aware of the 3 C's: content, contact and conduct?
- Does the online safety curriculum cover the full range of potential online risks which children may encounter?

Education

The 2020 edition has been updated to include new resources.

Action points:

- Have staff (subject leads, class teachers etc.) read and implemented guidance and appropriate curriculum resources in accordance with your local context e.g. age and ability of children?
    - How can you evidence this?

Protecting children

- This section has been retitled.

Governing bodies and proprietors **should** be doing all that they reasonably can to limit children's exposure to the above risks from the school or colleges IT system. As part of this process governing bodies and proprietors should ensure their school has appropriate filters and monitoring systems in place.

Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them a safe environment in which to learn, governing bodies and proprietors **should** consider the age range of their pupils, the number of pupils, how often they access the schools IT system and the proportionality of costs Vs risks.

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" might look like: UK Safer Internet Centre: appropriate filtering and monitoring.

- Governing bodies and proprietors should make informed decisions regarding the safety and security of the internet access and equipment available in their settings. Governing bodies and proprietors should ensure that the welfare of children and young people are paramount. Any decisions taken regarding filtering and monitoring systems should be taken from a safeguarding, educational and technical approach and should be justifiable and documented.
- When reviewing filtering and monitoring systems and approach some 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.
- The UK Safer internet Centre have put together guidance for settings 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.
- Settings should 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.
    - Kent settings using the KPSN Broadband system supported by EiS will be using the LightSpeed system, which has a range of tools to support settings in implementing appropriate filtering and monitoring systems.
    - Further information about LightSpeed can be accessed via EiS.
      Both Lightspeed and EiS have completed a response form for the UK Safer Internet Centre.

Action points:

- Does the leadership team understand the current filtering/monitoring systems in place within the setting?
    - 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, are the settings approaches to appropriate filtering and monitoring explicitly covered within the online safety and/or 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?
    - If so, how is this documented?
- Has the leadership accessed the UK Safer Internet centre (and any local guidance) material regarding appropriate filtering and monitoring?

Whilst filtering and monitoring is an important part of the online safety picture for schools and colleges to consider, it is only one part. Governors and proprietors should consider a whole school or college approach to online safety. This will include a clear policy on the use of mobile technology in the school or college. Many children have unlimited and unrestricted access to the internet via 3G, 4G and 5G in particular and the school and college should carefully consider how this is managed on their premises.

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 regards to online teaching and safeguarding.

- 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.
- It is vital for governing bodies, proprietors and members of staff to recognise that even with the most expensive and up-to-date security systems and filtering, children or staff can bypass them by using proxy sites or by using their own devices e.g. mobile phones or tablets which would not be subject to the settings filtering. Appropriate supervision, policy and procedures and education and training is essential.

- Schools and colleges should have a clear policy on the use of mobile technology in the school or college: Kelsi has specific content regarding the use of personal devices and mobile phones.

Action points:

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

Reviewing online safety

Technology in this area evolves and changes rapidly. A free online safety self-review tool for schools can be found via the 360 safe website. UKCIS has published 'Online safety in schools and colleges: Questions for the governing board' to help responsible bodies assure themselves that their online safety arraignments are effective.

- This section has been amended.

Action points:

- How do you evidence that your setting is reviewing and updating online safety practice regularly?

Education at home

Where children are being asked to learn online at home the department has provided advice to support schools and colleges do so safely: safeguarding-in-schools-colleges-and-other-providers and safeguarding-and-remote-education

- This is a new section added following the increased use of remote learning following the Covid-19 pandemic.
- The Education Safeguarding Service have published guidance and templates for educational settings to use following Covid-19 restrictions. We encourage DSLs and leaders to access the following:
    - Remote Learning Guidance
    - AUP for remote learning and communication
    - Online Safeguarding Resources for Educational Settings and Parents

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 89) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 93), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

- All members of staff should have access to appropriate, regular and up-to-date online safety information as part of their safeguarding training.
- 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.

- 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; all members of staff should be made aware of how to recognise, respond to, record and refer online safety concerns.
- The setting leadership team should also access training to ensure that messages are appropriate and consistent and to demonstrate to staff that safeguarding is a priority at the school.
    - Kent schools and colleges can access the Education Safeguarding Adviser (Online Protection) or the Online Safety Development Officer who provide centralised training, consultations and support for DSLs and bespoke whole staff training.

Action points:

- How does the setting provide all members of staff with appropriate and up-to-date training regarding online safety?
- Does staff training cover professional practice issues as well as safeguarding children?

Information and support

There is a wealth of information available to support schools, colleges and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point….

- The guidance links to a range of updated sources to help settings access additional support and resources.
    - The Education Safeguarding Adviser (Online Protection) and the Online Safety Development Officer are located within the Education Safeguarding Service; they provide educational settings in Kent with online safety advice, guidance and training.
    - Local information about online safety is provided for DSLs through the Education Safeguarding Team's 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?

Summary

The expanding role of technology to facilitate learning in a way many educational settings have not previously explored as a result of the Covid-19 pandemic means online safety is a key consideration for all educational settings.

The online safety agenda will continue to evolve and increase; it is essential that DSLs, governing bodies and proprietors are able to evidence that they recognise the importance of online safety within their statutory safeguarding responsibilities for all members of their community.

Schools and colleges should review their current online safety practice and implement any changes as required from 1st September 2020.

Kent educational settings can access specific online safety support and guidance via the Education Safeguarding Service.