Rebecca Avery, Education Safeguarding Adviser (Online Protection)
Education Safeguarding Team, Kent County Council
September 2016

Online Safety within 'Keeping Children Safe in Education' 2016: Information for Leaders and Managers

On the 26th May 2016 the Department for Education (DfE) published the updated 'Keeping children safe in education' guidance ready for implementation in September 2016. 'Keeping children safe in education' is statutory guidance from the DfE issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014 and the Non-Maintained Special Schools (England) Regulations 2015.

All schools and colleges must have regard to 'Keeping children safe in education' when carrying out their duties to safeguard and promote the welfare of children and schools and colleges should comply with the guidance unless exceptional circumstances arise.

'Keeping children safe in education' contains information on what schools and colleges should do and sets out the legal duties with which schools and colleges must comply in order to keep children safe. It should be read alongside statutory guidance 'Working together to safeguard children' and the DfE departmental advice 'What to do if you are worried a child is being abused – Advice for practitioners'.

This post will focus on elements of the document which are relevant to **online safety** and will be highlighting additions and changes regarding schools and colleges' statutory duties and responsibilities. It is recommended that Designated Safeguarding Leads (DSLs) read the entire document when looking at their current safeguarding practice and considering any required actions for September 2016.

Key Terms:

- 'School' describes all schools whether maintained, non-maintained or independent, including academies and free schools, alternative provision academies, maintained nursery schools and pupil referral units.
- 'College' describes all further education colleges and sixth-form colleges as established under the Further and Higher Education Act 1992, and relates to their responsibilities towards children under the age of 18, but excludes 16-19 academies and free schools (which are required to comply with relevant safeguarding legislation by virtue of their funding agreement).
- 'Staff' describes all members of staff working within a school or college setting including teaching and non-teaching staff and volunteers. This may include staff working on site even if they are not employed directly by the school/college for example catering staff etc.

How to read this document:

- Black font indicates a direct quote from the new guidance
- Blue font is used to highlight recommendations, best practice and useful links from the Kent County Council Education Safeguarding Adviser (Online Protection)
- Red font indicates a possible action point for DSLs, Governing bodies, Headteachers and proprietors to consider in readiness for September 2016.

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 and carers has a role to play in safeguarding children. (p.5)
    - This highlights that safeguarding and therefore online safety is identified as a responsibility for **all** members of staff in schools and colleges.

7. All school and college staff have a responsibility to provide a safe environment in which children can learn. (p.5)
    - This highlights that **all** members of staff have a responsibility to provide a safe environment in which children can learn, and this will include the online environment in which today's children now live and learn.

13. All staff members should receive appropriate safeguarding and child protection training which is regularly updated. In addition all staff members should receive safeguarding and child protection updates (for example, via email, e-bulletins and staff meetings), as required, but at least annually, to provide them with relevant skills and knowledge to safeguard children effectively. (p.6)
    - This will include school and college leaders ensuring that all members of staff access appropriate safeguarding training, which will need to include online safety.

Types of abuse and neglect

35. All school and college staff should be aware that abuse, neglect and safeguarding issues are rarely standalone events that can be covered by one definition or label. In most cases multiple issues will overlap with one another. (p.11)
    - This will include online safety abuse and safeguarding issues.

38. 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)… (p.11)
    - This specifically identifies that online or 'cyber' bullying can result in emotional abuse. It is therefore essential that schools anti-bullying policies are up-to-date and include schools approaches to dealing with all forms of bullying.
    - Kent County Council provides advice and guidance for schools and colleges regarding cyberbullying and responding to concerns and curriculum resources. The DfE preventing and tackling bullying guidance (which includes cyberbullying) can be found here.
    - Other useful documents include:
        - UK Safer Internet Centre
        - Childnet International

Action points

- Does our school/college anti-bullying policy identify cyberbullying and outline the school/college's response to any concerns reported?

39. Sexual abuse: involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving a high level of violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing and touching outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse (including via the internet). Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children. (p.11)
    - This specifically identifies that sexual abuse can occur via the internet and can involve a range of activities, including but not limited to online grooming and exploitation, exposure to pornographic content and engaging a child in sexual activity online.
    - This also identifies that perpetrators can be male or female and may include children themselves (such as in cases of sexting). Schools and colleges must ensure that safeguarding and child protection policies and procedures cover online sexual abuse.
    - Kent County Council provides an Online Safety Policy template and guidance as part of our Safeguarding Policies templates and also template Acceptable Use Policies which can be used by schools and colleges to develop staff behaviour policy which is relevant to their own needs.
    - Other useful links to access template policy documents include:
        - UK Safer Internet Centre
        - Childnet International
        - South West Grid for Learning
        - London Grid for Learning
        - Northern Grid (Digitally Confident)

Action point:

- Does our school/college safeguarding and child protection policy clearly identify the use of technology as a potential risk to members of the community?

Specific safeguarding issues

41. All staff should have an awareness of safeguarding issues… Staff should be aware that behaviours linked to the likes of …. sexting puts children in danger. (p.12)
    - All members of staff must be aware of range of safeguarding issues, and specifically highlights the need for staff to be aware of sexting. Sexting can be defined as 'an increasingly common activity among children and young people, where they share inappropriate or explicit images online…'. This can include sharing indecent images of themselves or others via mobile phones, webcams, social media and instant messaging.
    - Although viewed by many young people as 'normal' and part of 'flirting', by sending an explicit image, a young person is producing and distributing child abuse images and risks being prosecuted, even if the picture is taken and shared with their permission. They can also be at increased risk of blackmail, bullying, emotional distress and unwanted attention. Whilst it is usually more common with teenagers, sexting behaviour can impact on younger children, for example risk taking behaviour or natural curiosity so all schools must consider how to respond. (NSPCC)
    - Sexting is likely to be an issue which could be highlighted within staff safeguarding training. DSLs should also take action to ensure that all members of staff know how to

respond to sexting concerns appropriately and in line with the school/college policy e.g. confiscate devices and report concerns to the DSL immediately. For example, are all members of staff aware that if a child discloses they have sent or received a "sext" then these images should not be printed, copied or forwarded.

- Kent County Council includes links to national guidance and support regarding responding to sexting within the Online Safety Policy template and guidance. The KSCB procedures also include responding to harmful behaviours and underage sexual activity. More guidance regarding sexting will be published by the KSCB in line with national guidance when it is made available.
- Useful links regarding responding to sexting:
    - UK Safer Internet Centre
    - Childnet – Sexting and the Law
    - Childnet – Hot Topic – Sexting
    - Childnet – "Picture this" resource
    - Spirto Resources
    - SWGfL – "So you got naked online" booklet
    - Think U Know 14+
    - Think U Know 11-13
    - NSPCC -Share Aware Resources
    - Parents Info – what is and isn't legal
    - ChildLine
    - ChildLine – Zipit app
    - UKCCIS Sexting Guidance for schools and colleges

Action point:

- Does our school/college policies identify sexting as a possible risk for children?
- Does our school/college provide training and appropriate information to members of staff regarding identifying concerning behaviours which may be linked to sexting?

42. All staff should be aware safeguarding issues can manifest themselves via peer on peer abuse. This is most likely to include, but not limited to: bullying (including cyber bullying), gender based violence/sexual assaults and sexting. Staff should be clear as to the school or college's policy and procedures with regards to peer on peer abuse. (p.12)
    - This specifically highlights that all members of staff must be advised that abuse can also be perpetrated by children themselves and again specifically highlights cyberbullying and. Training should ensure that all members of staff are aware that not all online abuse is committed by strangers and the education provided to children should reflect this.

Action point:

- Does our school/college provide training to members of staff regarding peer on peer abuse, including cyberbullying and sexting?

43. Expert and professional organisations are best placed to provide up-to-date guidance and practical support on specific safeguarding issues. …bullying including cyberbullying… child sexual exploitation (CSE) and Annex A….preventing radicalisation – and Annex A….sexting.(p.12)
    - This specifically highlights specific forms of online abuse.

43. Annex A contains important additional information about specific forms of abuse and safeguarding issues. School leaders and those staff that work directly with children should read the annex. (p.13)
    - Annex A specifically highlights forms of abuse which may involve the internet, including Child Sexual Exploitation (CSE) and radicalisation.

Part two: The management of safeguarding

Legislation and the law

45. Governing bodies and proprietors (in Part two unless otherwise stated this includes management committees) must ensure that they comply with their duties under legislation. They must have regard to this guidance to ensure that the policies, procedures and training in their schools or colleges are effective and comply with the law at all times (p.15)
    - This will include ensuring that governing bodies and proprietors are aware of relevant legislation with regards to online safety concerns. Further information about some of the relevant legislation can be found within the Kent Online Safety Policy template and guidance.

Action Point:
- Do our school/college leaders have an understanding of the relevant legislation which applies to online safeguarding?

Safeguarding policies

47. 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. (p.14)

48. This should include:
- an effective child protection policy; and
- 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. (p.14-15)
  This is not intended to be an exhaustive list. These policies, along with Part one of this guidance (Keeping children safe in education) and information regarding the role of the designated safeguarding lead, should be provided to all staff on induction. (p.15)
  - This highlights the need for schools and colleges to have robust safeguarding policies, including a staff behaviour policy, which covers the school's expectations and approaches towards online safety and also regarding professional online practice. This will include child protection and safeguarding policies and the staff behaviour policy.
  - All members of staff will need to have read and understood the relevant online safety policies and procedures, and we would recommend that this is provided to all members of staff (including volunteers) as part of induction and that these policies are updated and shared with staff on a regular (at least annual) basis.
  - Kent County Council provides an Online Safety Policy template and guidance as part of our Safeguarding Policies templates and also provides template Acceptable Use Policies which can

be used by schools and colleges to develop a staff behaviour policy which is relevant to their own needs and requirements.

- Other useful links to access template policy documents include:
  - UK Safer Internet Centre
  - Childnet International
  - South West Grid for Learning
  - London Grid for Learning
  - Northern Grid (Digitally Confident)

Action Point:

- Does our school/college child protection policy include online safety (either within the policy itself or references a separate online safety policy)?
- Does our school/college staff behaviour policy (or code of conduct or Acceptable Use Policy) cover the acceptable use of technology, including communication via social media?
- How do we ensure that this information is communicated with and understood by all members of staff?
- How do we communicate any changes or updates in our policies with staff?

The designated safeguarding lead

52. Governing bodies and proprietors should appoint an appropriate senior member of staff, from the school or college leadership team, to the role of designated safeguarding lead. The designated safeguarding lead should take lead responsibility for safeguarding and child protection. (p.15)
53. It is a matter for individual schools and colleges as to whether they choose to have one or more deputy designated safeguarding lead(s). Any deputies should be trained to the same standard as the designated safeguarding lead. (p.15)
54. 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. (p.15)
55. The designated safeguarding lead and any deputies should liaise with the local authority and work with other agencies in line with Working together to safeguard children. (p.15)
56. The designated safeguarding lead and any deputies should undergo training to provide them with the knowledge and skills required to carry out the role. The training should be updated every two years. (p.15-16)
57. In addition to their formal training, as set out above, 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, but at least annually, to keep up with any developments relevant to their role. (p.16)
    - The ultimate responsibility for online safety falls within the remit of the Designated Safeguarding Lead (DSL) as online safety is a safeguarding issue. Some schools and colleges may delegate some of the activities regarding online safety to other members of staff, for example due to individual knowledge and experience, especially regarding curriculum content or specific technical knowledge and skills.
    - As online safety is clearly identified as a safeguarding priority it will not be appropriate for the online safety lead to be another member of staff, for example a computing lead, unless they have also accessed appropriate training (e.g. DSL training).

- Staff with appropriate skills, interest and expertise regarding online safety should be encouraged to help support the DSL(s) as appropriate, for example when developing curriculum approaches or making technical decisions. However schools and colleges must be clear that ultimate responsibility for online safety sits with the Designated Safeguarding Lead.
- It is important that DSLs access appropriate online safety training to ensure they are aware of the specific online concerns which children, young people and adults may encounter and are able to take appropriate steps to ensure that practice in their settings is in line with national and local policy and procedures.
- In Kent, specific training for DSL is available via Kent CPD online. Information about online safety is also provided for DSLs through the Kelsi e-Bulletin, the Education Safeguarding Team's Child Protection Newsletter, the e-Safety pages on Kelsi, the Kent e-Safety Twitter feed and the Kent e-Safety blog. DSLs are able to access specific online safety consultations via the Education Safeguarding Adviser (Online Protection) and e-Safety Development Officer.

Action Point:

- Is the school/college DSL considered to be the lead person responsible for online safety?
  - If not, have any other persons responsible had appropriate training to enable them to support the DSL?
- If appropriate, has the school identified other members of staff who may have skills, expertise or interests that may enable them to support the DSL?
  - If so, who are they and have they had appropriate training to enable them to support the DSL?
- Has the DSL (and any other appropriate members of staff as identified by the school/college) had appropriate training to enable them to respond to online safety concern?
  - Does this training include developing an up-to-date awareness of both risks and benefits of technology and an awareness of both national and local policy and procedures.
  -

Staff training

64. Governing bodies and proprietors should ensure that all staff members undergo safeguarding and child protection training at induction. The training should be regularly updated. Induction and training should be in line with advice from the LSCB. (p.17)
65. In addition all staff members should receive regular safeguarding and child protection updates (for example, via email, e-bulletins, staff meetings), as required, but at least annually, to provide them with relevant skills and knowledge to safeguard children effectively. (p.17)
66. 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 child protection policy. (p.17)
    - Safeguarding and child protection training provided to staff, on induction (and at least annually), should include online safety. This is highlighted further in annex C.
    - Schools and colleges may wish to integrate online safety within current safeguarding and child protection training or provide separate and specific sessions. Some good practice examples identified within Kent include schools and college which cover safeguarding (including online safety) as a standing item at all staff meetings and

schools and colleges which provide specific online safety trainings sessions as part of an annual staff training calendar of events.

- Staff should be involved in the development and construction of online safety (including acceptable use policies) policies to promote ownership and understanding. This may involve including staff in development via discussions at staff meetings or reviewing policies with staff working groups.
- (Also see the section on staff training as highlighted within Annex C)

Action Point:

- How does our school/college provide appropriate, up-to-date and relevant whole staff training which includes online safety?
- How does our school/college involve staff in developing and contributing to online safety policies and procedures?

Online safety

67. 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 is provided in Annex C.

- This identifies that online safety is viewed as part of schools and colleges safeguarding responsibilities. This should encourage schools and colleges to recognise the increasing role of the internet within safeguarding and child protection concerns as well as the need to ensure appropriate systems are in place to filter and monitor internet activity.
- The UKCCIS Education Group has developed guidance for school governors to help governing boards support their DSL to keep children safe online. Governors can use this document to: gain a basic understanding of the school's 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. The document includes examples of good and outstanding practice, as well as identifying when governors should be concerned.

Action point:

- Does our school/college clearly view online safety as a safeguarding concern?
- Has our DSL, governing body/proprietor etc. read and understood annex C?
- Have the Governor's accessed the UKCCIS online safety for school Governors guidance?
    - Can this document be used to help provide evidence of strategic Governor oversight?

Opportunities to teach safeguarding

68. Governing bodies and proprietors should ensure children are taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum. This may include covering relevant issues through personal, social, health and economic education (PSHE), tutorials (in FE colleges) and/or – for maintained schools and colleges – through sex and relationship education (SRE). (p.17-18)

- Governing bodies and proprietors should ensure that online safety is specifically covering within the curriculum. The responsibility for teaching children about online

safety is clearly identified as not being the sole responsibility of the computing curriculum and therefore must be woven throughout the curriculum. Online safety education should start within early years and be developed throughout the year and across all age groups.

- One-off events, lessons or assemblies regarding online safety or a reliance on external speakers to educate children will not be effective or adequate practice. External speakers can be useful as a catalyst to a discussion or to reinforce learning but cannot be the sole source of education or sanction for children, as they will not be effective in the long-term or enable schools and colleges to develop internal capacity to respond to concerns.
- Online safety education may occur explicitly, such as within specific lessons in PSHE and computing, however it should also be taught discreetly. It is recommended that schools and colleges ensure that all members of staff consider how online safety can be taught within their own curriculum or subject, for example when other subjects use technology as a teaching and learning tool. It is good practice for all staff to reference ways in which safeguarding and online safety can be reinforced and developed within their lesson plans.
- The school/college online safety curriculum should be flexible, relevant and engage pupils' interests, be appropriate to their own needs and abilities and encourage them to develop resilience to online risks. Schools and colleges should ensure they use a range of relevant resources and be mindful that online safety educate content can date very quickly due to the rapid pace of change within technology.
- Best practice would involve schools and colleges ensuring learners have an input into the online safety curriculum, this could involve use of student/pupil councils or use of peer education approaches.
- The SWGfL and Common sense media have produced a progressive digital literacy scheme of work which may be useful to enable schools and colleges. Childnet have identified ways to teach online safety within the computing curriculum.
- The Kent Education Safeguarding Adviser (Online Protection) and e-Safety Development Officer have compiled a list of a range of curriculum resources for schools and colleges here.

Action point:

- How does our school/college current teach children about online safety?
  - Are all year groups receiving online safety education that is relevant, up-to-date and appropriate to them?
  - Is there a clear scheme of work which identifies relevant and appropriate teaching resources?
- Is the online safety curriculum differentiated to our learners needs, ages and abilities?
- How does the school/college identify and target children who may require more specific educational approaches to enable them to build online safety skills?
- How are children and young people involved in the development of the online safety curriculum?
- Is the online safety curriculum integrated throughout the academic year?
- Is the online safety curriculum integrated throughout all subject areas?
- How does our school/college use external speakers to complement our own internal education approaches?

69. 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. (p.18)
    - Governing bodies and proprietors should be making informed decision regarding filtering and monitoring systems and ensure decisions are appropriate to the school's technology provision as well as the needs of the learners. A reliance on filtering to safeguarding children will not be appropriate, and children will need to be taught critical thinking skills which are appropriate to their age and ability.
    - Schools and colleges may wish to consider developing a risk assessment approach or other process to ensure filtering decisions are made from a safeguarding, technical and educational perspective.
    - The UK Safer internet Centre have put together excellent guidance for schools and colleges about appropriate filtering and monitoring and it is recommended that governing bodies and proprietors read this guidance fully.

Action point:

- How does the governing body/proprietor make informed decisions regarding the school/college filtering and monitoring systems and associated decisions?
    - How is this captured and recorded?

Inspection

70. From September 2015 all inspections by Ofsted have been made under: A new common inspection framework: education, skills and early years. Inspectors will always report on whether or not arrangements for safeguarding children and learners are effective. Ofsted has published a document setting out the approach inspectors should take to inspecting safeguarding: Inspecting safeguarding in early years, education and skills settings. Individual inspectorates will also report on safeguarding arrangements and have published frameworks which inform how they inspect the independent schools that are not inspected by Ofsted at: School Inspection Service and Independent Schools Inspectorate. (p.18)
    1. The Ofsted Common Inspection Framework and supporting "Inspecting Safeguarding" document specifically highlights online safety. Additional guidance regarding this (updated in August 2016) can be found here.
    2. Schools/colleges may wish to audit current practice to identify strengths and areas for improvement. Tools which may be helpful to support schools and colleges will include the 360 safe tool and the Kent self-evaluation document.

Action point:

- Are all members of staff (especially leadership staff) aware of online safety within the Ofsted Common Inspection Framework?
- Has the school/college reviewed current practice and identified areas for improvement?

Allegations of abuse made against other children

76. Staff should recognise that children are capable of abusing their peers. Governing bodies and proprietors should ensure their child protection policy includes procedures to minimise the risk of peer on peer abuse and sets out how allegations of peer on peer abuse will be investigated and

dealt with. The policy should reflect the different forms peer on peer abuse can take, make clear that abuse is abuse and should never be tolerated or passed off as "banter" or "part of growing up". It should be clear as to how victims of peer on peer abuse will be supported. (p.19)

77. Peer on peer abuse can manifest itself in many ways. Governors and proprietors should ensure sexting and the school or colleges approach to it is reflected in the child protection policy. The department provides searching screening and confiscation advice for schools (link). Child Exploitation Online Protection Centre (CEOP) has recently updated their sexting guidance: Sexting in Schools and Colleges. (p.19)

- This identifies that abuse can be perpetrated by children. It specifically highlights the need for governors and proprietors to ensure that schools and colleges safeguarding and child protection policies include responding to sexting concerns. This is essential to safeguard children and staff and also to ensure that any criminal investigations are undertaken promptly and appropriately and also to ensure that Local Safeguarding Children Board and child protection procedures are followed.
- Kent County Council provides an online safety advice, including policy template and guidance which covers responding to sexting concerns. The Kent Safeguarding Children Board specifically highlights sexting within its procedures. The Kent Safeguarding Children Board has published a short guide and flowchart for Kent professionals to use to respond locally to youth produced sexual imagery concerns (otherwise known as sexting). This document should be used to help inform the decision making of Designated Safeguarding Leads when responding to concerns. A flowchart and two page guidance summary can be accessed on the KSCB website
- DSLs can also access the Education Safeguarding Team for advice and guidance regarding responding to sexting concerns. A selection of useful resources regarding sexting are highlighted within the "specific safeguarding issues" section above.
- DSLs should ensure they are familiar with local KCSB and national UKCCIS guidance.

Action point:

- Is the DSL familiar with local and national guidance for responding to allegations of abuse against other children?
    - How has the DSL communicated this information to other members of staff?

Annex A: Further information

Further information on child sexual exploitation

Child sexual exploitation is a form of sexual abuse where children are sexually exploited for money, power or status. It can involve violent, humiliating and degrading sexual assaults. In some cases, young people are persuaded or forced into exchanging sexual activity for money, drugs, gifts, affection or status. Consent cannot be given, even where a child may believe they are voluntarily engaging in sexual activity with the person who is exploiting them. Child sexual exploitation does not always involve physical contact and can happen online… (p.52-53)

- Child sexual exploitation (CSE) may involve the role of the internet to identify potential victims or as a tool to coerce and blackmail children into performing sexual acts, both on and offline. The internet may also be provided to children as a "gift" by perpetrators, for example in the form of new mobile phones and devices. In some cases CSE can entirely take place online, for example children being coerced into performing sexual acts via webcam, and may not always

result in a physical meeting between children and the offender. DSLs should be aware of national and local policy and procedures regarding CSE.

- The Kent County Council online safety policy template and guidance covers responding to online CSE concerns. Further information about local approaches, including the CSET team and Operation Willow is available. The KSCB CSE toolkit is available to enable DSLs to consider possible risks. Multi-agency CSE training is also available via the KSCB.

Action point:

- Does the safeguarding and child protection policy include responding to the risk of CSE?
  - Does this include the use of technology as a tool for CSE within all appropriate policies?
- Has the DSL had appropriate training regarding CSE?
- How does the DSL communicate awareness and understanding of CSE (including online CSE) to staff?
- How are children educated to be aware of CSE (including online CSE) appropriately to their age and ability?

Further information on preventing radicalisation

Protecting children from the risk of radicalisation should be seen as part of schools' and colleges' wider safeguarding duties, and is similar in nature to protecting children from other forms of harm and abuse. During the process of radicalisation it is possible to intervene to prevent vulnerable people being radicalised. (p.54-55)

Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism. There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. It can happen in many different ways and settings. Specific background factors may contribute to vulnerability which are often combined with specific influences such as family, friends or online, and with specific needs for which an extremist or terrorist group may appear to provide an answer. The internet and the use of social media in particular has become a major factor in the radicalisation of young people. (p.55)

Schools must ensure that children are safe from terrorist and extremist material when accessing the internet in schools. (p.56)

- This highlights the role of the internet as a tool in the radicalisation of young people and also in the potential accidental and deliberate exposure of young people and adults to extremism views and content. This section highlights that procedures for responding to radicalisation may be set out in existing safeguarding policies and separate policies are not necessary. DSLs should be aware of national and local policy and procedures regarding radicalisation.
- The Kent County Council Safeguarding and Child Protection Policy template and online safety policy template and guidance covers responding to radicalisation concerns. Further information about Prevent Duty and the Kent approach (including procedures, tools and training) can be found on Kelsi .
- The Department for Education has also published advice for schools 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.

Action point:

- Does the safeguarding and child protection policy include responding to the risk of radicalisation?
    - Does this include the use of technology as a tool for radicalisation within all appropriate policies?
- Has the DSL had appropriate training regarding radicalisation and Prevent?
- How does the DSL communicate awareness and understanding of radicalisation (including online) to staff?
- How are children educated to be aware of radicalisation (including online) appropriately to their age and ability?

Annex B: Role of the designated safeguarding lead

This section (p.58-60) highlights the roles and responsibilities of the DSL(s) including managing referrals, multi-agency working, training, record keeping, awareness raising and availability. These roles and responsibilities will also apply to online safety concerns, especially as some online issues may require referral to other agencies and schools/colleges will need to raise awareness of recognising, responding, recording and referring online safeguarding issues with all members of staff.

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. (p.61)

- This clearly identifies online safety as a safeguarding responsibility and highlights the need for schools and colleges to ensure that all members of their communities are able to 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
contact: being subjected to harmful online interaction with other users
conduct: personal online behaviour that increases the likelihood of, or causes, harm (p.61)

- It is essential that schools and colleges develop a curriculum that is appropriate to the needs of their learners and that which covers a range of online safety issues (e.g. not just covering “grooming” by strangers). Online safety messages shared with staff and children should be appropriate and up-to-date and empower them to be able to respond to a range of online threats as well as opportunities.

Action point:

- Does the online safety curriculum cover the full range of potential online risks which children may encounter?

Filters and monitoring

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
Guidance on e-security is available from the National Education network (NEN). Buying advice for schools is available here: buying for schools. (p.61)

- Governing bodies and proprietors must make informed decisions regarding the safety and security of the internet access and equipment available in their settings. Governing bodies and proprietors must ensure that the welfare of children and young people is paramount at all times. 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 excellent guidance for schools and colleges 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.
- Schools may also wish to approach their broadband provider to consider the range of tools available to them which may enable them to develop strategies to control and supervise their internet use and systems appropriately. Kent schools and settings using the EIS School Broadband system will be using the LightSpeed system which already has a range of tools which may enable schools to be able to demonstrate they have an understanding of appropriate filtering and monitoring and have systems already in place. 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 point:

- Does the Headteacher/governing body/proprietor understand the current school/college filtering/monitoring systems?
    - If not, how can this be developed?

- How do the gHeadteacher/governing body/proprietor 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 Headteacher/governing body/proprietor accessed the UK Safer Internet centre (and any local guidance) material regarding appropriate filtering and monitoring?

Whilst filtering and monitoring are 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 approach to online safety. This will include a clear policy on the use of mobile technology in the school. Many children have unlimited and unrestricted access to the internet via 3G and 4G in particular and the school and college should carefully consider how this is managed on their premises. (p.61-2)

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. (p.62)

- No filtering or monitoring solution can offer schools and colleges 100% protection from exposure to inappropriate or illegal content, so it is equally important that they can demonstrate that they have taken all other reasonable precautions to safeguard children and staff. Such methods may include appropriate supervision, requiring children and staff to sign an acceptable Use Policy (AUP), a robust and embedded online safety curriculum and appropriate and up-to-date staff training etc. A reliance on filtering and monitoring to safeguarding children online could lead to a feeling of complacency which may put children and adults at risk of significant harm.
- It is vital for all 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 potentially bypass them either via using proxy sites or by using their own devices e.g. mobile phones or tablets which would not be subject to the school/colleges filtering. This is why appropriate supervision, policy and procedures and education and training is essential. The Kent County Council online safety policy template and guidance has specific content for schools and colleges regarding filtering and also use of personal devices and mobile phones.

Action point:

- Does the school/college understand that filtering and monitoring will not always be effective as removing risk?
- How do all members of staff ensure that technology in the classroom is used as safely and effectively as possible?
    - Does the school 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 school/college have a policy regarding safe and appropriate use of mobile phones and personal devices?

Staff training

Governors and proprietors should ensure that as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 64) and the requirement to ensure children are taught about safeguarding, including online (paragraph 68), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach. (p.62)

- This identifies that all members of staff must have access to appropriate, regular and up-to-date online safety training as part of their safeguarding training. Schools and colleges will need to consider how this is implemented within their own settings (e.g. integrated within existing safeguarding and child protection training or as separate and specific online safety training).
- Frequently during online safety training provided by the Education Safeguarding team, school leaders and non-teaching staff are absent. Whilst ensuring a whole staff group presence is difficult due to demands on time, resources and other commitments, a failure to identify online safety as a whole school issue could potentially undermine the school/colleges safeguarding practice, ultimately leaving children and adults vulnerable.
- 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 (including external staff and volunteers) should be made aware of how to recognise, respond to, record and referral all safeguarding concerns, including online issues. School leaders must also access this training to ensure that messages are appropriate and consistent and also to demonstrate to staff that safeguarding is a key propriety at the school.
- Kent schools and colleges can access the Education Safeguarding Adviser (Online Protection) or the e-Safety Development Officer who provide centralised training as well as consultations and support for DSLs or can provide schools and colleges with bespoke whole staff training. Kent DSLs can access a template presentation via Education Safeguarding Adviser (Online Protection) or the e-Safety Development Officer to use as part of staff training.
- Other useful links to support staff training include:
    - Childnet – Inset presentation
    - Childnet – Guidance for working with young people
    - Childnet – Guidance for you as a professional
    - Childnet – Professional Reputation
    - UK Safer Internet Centre – Professional Reputation
    - UK Safer Internet Centre Helpline
    - UK Safer Internet Centre Helpline FAQs
    - KSCB – Safer Practice with Technology

Action point:

- How does the school/college provide all members of staff with appropriate and up-to-date training regarding online safety?
    - If so, is it embedded within safeguarding training or is it separate and specific?
    - Is it provided to ALL members of staff, including non-teaching staff, school leaders and volunteers?
- Does staff training cover safeguarding children online as well as expectations for professional practice?

Information and support

There is a wealth of information available to support schools and colleges to keep children safe online. The following is not exhaustive but should provide a useful starting point:

- www.thinkuknow.co.uk
- www.disrespectnobody.co.uk
- www.saferinternet.org.uk
- www.internetmatters.org
- www.pshe-association.org.uk
- www.educateagainsthate.com
- www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation (p.62)

- The Education Safeguarding Adviser (Online Protection) and the e-Safety Development Officer are located within the Kent County Council Education safeguarding Team and provide schools with advice, guidance and training regarding online safety.
- Information about online safety is also provided for DSLs through the Kelsi e-Bulletin, theEducation Safeguarding Team's Child Protection Newsletter, the e-Safety pages on Kelsi, the Kent e-Safety Twitter feed and the Kent e-Safety blog.
- Kent schools and colleges can contact the Education safeguarding Adviser (Online Protection) and e-Safety Development Officer directly for advice, support and guidance regarding online safety.

Action point:

- How does the school/college (specially the DSL) keep up-to-date with developments within the online safety agenda?

Summary

The online safety agenda has evolved significantly over recent years and it is essential that schools and colleges (especially DSLs, governing bodies and proprietors) recognise the role of online safety within their safeguarding responsibilities towards all members of the community.

It is essential that schools and colleges review their current online safety practice and consider changes required to be in place since September 2016.

Kent schools and colleges can access the Education Safeguarding Team if they require further support and guidance.