Rebecca Avery, Education Safeguarding Adviser (Online Protection)
Education Safeguarding Team, Kent County Council/The Education People
May 2018

Online Safety within 'Keeping Children Safe in Education' 2018

On the 17th May 2018 the Department for Education (DfE) published the updated 'Keeping children safe in education' (KCSIE) guidance ready for implementation from the 3rd September 2018. Schools and Colleges must comply with KCSIE 2016 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; schools and colleges should comply with the guidance unless exceptional circumstances arise.

This document focuses on elements of KCSIE 2018 relevant to **online safety**; it will also highlight additions and changes from KCSIE 2016. It is recommended that DSLs and leaders read the entire KCSIE 2018 document when evaluating their current safeguarding practice and considering required actions for September 2018. The NSPCC have produced a briefing which explores key changes.

This document has been written for Designated Safeguarding Leads (DSLs) and educational setting leadership teams by Rebecca Avery, Education Safeguarding Adviser (Online Protection) within the Education Safeguarding Team. Additional guidance and resources relating to online safety can be found at: www.kelsi.org.uk/child-protection-and-safeguarding/e-safety

Summary of key changes related to online safety:

- All staff should undergo safeguarding and child protection training (including online safety) at induction
- The updated guidance includes a new section (Part 5) on child on child sexual violence and sexual harassment, which can occur both on and offline
- New or more detailed information on safeguarding issues is provided; this includes online issues
- Online safety is specifically referenced as part of the responsibility for the DSL within Annex B; The role of the DSL
- There is an expectation that DSLs will access appropriate training to ensure they are able to understand the unique risks associated with online safety, can recognise the additional risks that children with SEN and disabilities (SEND) face online, and have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- Additional links have been added to supporting materials in annex C, online safety; this includes references to tools to assist settings in reviewing their online safety practice

How to read this document:

- This font indicates a direct quote from the KCSIE 2018 guidance
- This font indicates content has been added or amended since KCSIE 2016
- This font is used to highlight recommendations, good practice and useful links
- This font indicates a possible action points for DSLs, Governing bodies, Headteachers and proprietors to consider in readiness for September 2018.

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 this guidance.

Part one: Safeguarding information for all staff

What school and college staff should know and do (p5-8)

2. Safeguarding and promoting the welfare of children is everyone's responsibility…

    - Safeguarding (therefore online safety), is identified as a responsibility for **all** members of staff.

7. All school and college staff have a responsibility to provide a safe environment in which children can learn.
    - This should include the online environment.

13. **All** staff **should** be aware of systems within their school or college which support safeguarding, and these should be explained to them as part of staff induction. This **should** include: the child protection policy; the behaviour policy; the staff behaviour policy (sometimes called a code of conduct) …; and the role of the designated safeguarding lead (including the identity of the designated safeguarding lead and any deputies).
    - This should include online safety.
        - Kent County Council provides an Online Safety Policy template and guidance as part of our safeguarding policies templates.
        - Other useful links to access template policy documents include:
            - UK Safer Internet Centre
            - Childnet International
            - South West Grid for Learning
            - London Grid for Learning

14. All staff **should** receive appropriate safeguarding and child protection training which is regularly updated. In addition, all staff **should** receive safeguarding and child protection updates (for example, via email, e-bulletins and staff meetings), as required, and at least annually, to provide them with relevant skills and knowledge to safeguard children effectively.
    - This should include online safety.

17. All staff **should** know what to do if a child tells them he/she is being abused or neglected…
    - This should include online safety.

What school and college staff should look out for (p8)

19. All staff **should** be aware of indicators of abuse and neglect so that they are able to identify cases of children who may be in need of help or protection. Indicators of abuse and neglect, and examples of safeguarding issues are described in paragraphs 43-53 of this guidance.
    - This should include online safety abuse and safeguarding issues.

Indicators of abuse and neglect (p14)

46. 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 result in emotional abuse. Anti-bullying policies should be up-to-date and include the settings approaches to dealing with all forms of bullying, including cyberbullying.
    - Kent County Council provides advice and guidance for educational settings regarding cyberbullying, responding to concerns as well as links to 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 anti-bullying policy include cyberbullying?
- Does our policy outline the procures to follow when cyberbullying concerns are reported?

47. 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 … 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 activities.

Action points

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

Specific safeguarding issues (p15)

49. 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.

50. 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) …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 sexting and cyberbullying.

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

- DSLs should ensure all members of staff know how to respond to 'sexting' concerns appropriately. For example, are staff aware that if a child discloses they have sent or received a potentially indecent image, these images should not be printed, copied or forwarded.

52. Safeguarding incidents and/or behaviours can be associated with factors outside the school or college and/or can occur between children outside the school or college....
    - This is especially likely to be the case with regards to online safety concerns.

53. Annex A contains important additional information about specific forms of abuse and safeguarding issues. School and college leaders and those staff who work directly with children **should** read the annex.

Action points:
- Do we provide sufficient training to members of staff regarding peer on peer abuse, including cyberbullying and sexting?
- Do our policies identify sexting (youth produced sexual imagery) as a possible risk for children?
- Do we provide appropriate training and information to members of staff regarding identifying concerning behaviours which may be linked to sexting and cyberbullying?

Part two: The management of safeguarding

Legislation and the law (p16)

54. Governing bodies and proprietors … **must** ensure that they comply with their duties under legislation. They **must** have regard to this guidance, ensuring that policies, procedures and training in their schools or colleges are effective and comply with the law at all times.
    - This should 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 points:
- Does our leadership team have a sufficient understanding of the relevant legislation which applies to online safeguarding?

Safeguarding policies (p16-17)

56. 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.

57. 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.
        - This highlights the need for individual settings to have specific and robust safeguarding policies, updated at least annually, that are publicly available. If settings do not have a stand-alone online safety policy, relevant information should be integrated into the relevant child protection policies.
    - 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.

58. ...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.

- The staff behaviour policy should cover the settings expectations regarding professional conduct online; all members of staff need to be provided with this information as part of induction. Settings should ensure all staff have read and understood the relevant online safety policies and procedures; which should be updated (at least annually) and shared with staff on a regular basis.
- Kent County Council provide an online safety policy template and guidance as part of our safeguarding policies templates; template Acceptable Use Policies (AUPs) are also available to be used to develop a staff behaviour policy relevant to settings specific needs and requirements.
- Other useful links for template policy documents include:
    - UK Safer Internet Centre
    - Childnet International
    - South West Grid for Learning
    - London Grid for Learning

Action points:

- Does our child protection policy include 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 our staff behaviour policy (code of conduct/Acceptable Use Policy) cover the acceptable use of technology for staff, 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 and updates in our policies with staff?

The designated safeguarding lead (p18)

61. Governing bodies and proprietors **should** ensure an appropriate **senior member of staff**, from the school or college **leadership team**, is appointed to the role of designated safeguarding lead. The designated safeguarding lead **should** take **lead responsibility** for safeguarding and child protection…

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

63. 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.

- As online safety is identified as a safeguarding issue, the ultimate responsibility 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 must be clear that ultimate responsibility for online safety sits with the DSL.

Action points:

- Is the settings DSL the lead person responsible for online safety?
- Has the school identified other members of staff who have skills, expertise or interests that enable them to support the DSL?
    - If so, have they had appropriate training to enable them to act as a deputy DSL?

Staff training (p21-22)

76. 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 LSCB.
    - Child protection training, including online safety should be provided to all staff on induction. Settings should also consider how online safety is covered within the 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.
    - 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.

Action points:

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

Online safety (p.21)

79. 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.
    - Online safety is clearly viewed as part of settings safeguarding responsibilities; this should encourage settings to recognise the role of the internet within child protection concerns, as well as ensuring 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 settings current approach to keeping children safe online; learn how to improve this approach where appropriate; and find out about tools which can be used to improve the approach. It includes examples of good and outstanding practice, as well as when governors should be concerned.

Action points:

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

Opportunities to teach safeguarding (p21)

80. 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.

81. This may include covering relevant issues through Relationships Education and Relationships and Sex Education (also known as Sex and Relationship Education), tutorials (in colleges) and/or where delivered, through Personal, Social, Health and Economic (PSHE) education.

82. 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 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 be woven throughout the curriculum 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 are unlikely to be successful if they are the the sole source of education or sanctions; in some cases this approach can undermine settings ability to develop internal capacity to respond to concerns.
        - UKCCIS have published guidance for educational settings regarding the use of external visitors.
    - Online safety education may occur explicitly, such as within specific lessons in PSHE and computing, however it should also be taught discreetly. Staff should consider how online safety can be taught within all subjects whenever technology is used a teaching and learning tool.
- The 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.
    - Settings 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.
    - Good practice is to gain learner input into the online safety curriculum; this could involve use of student/pupil councils or use of peer education approaches.
- The UKCCIS education working group have published the 'Education for a connected world' framework to help settings consider appropriate skills and knowledge required

- The SWGfL and 'Common Sense Media' have produced a progressive digital literacy scheme of work which may be useful. Childnet have also 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 educational settings here.

Action points:

- How does our setting currently teach children and young people about online safety?
  - Are all year groups receiving 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 our setting 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 curriculum?
- Is the curriculum integrated throughout the academic year and across subject areas?
- How does our setting use external speakers to complement our own internal education approaches?

Peer on peer abuse (p22-23)

89. **All** staff **should** recognise that children are capable of abusing their peers. All staff **should** be clear about their school or college's policy and procedures with regard to peer on peer abuse.

90. Governing bodies and proprietors **should** ensure that their child protection policy includes: procedures to minimise the risk of peer on peer abuse; how allegations of peer on peer abuse will be recorded, investigated and dealt with; clear processes as to how victims, perpetrators and any other child affected by peer on peer abuse will be supported; a clear statement that abuse is abuse and should never be tolerated or passed off as "banter", "just having a laugh" or "part of growing up"; recognition of the gendered nature of peer on peer abuse (i.e. that it is more likely that girls will be victims and boys perpetrators), but that all peer on peer abuse is unacceptable and will be taken seriously; and the 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 Child Internet Safety (UKCCIS) Education Group has published advice for schools and colleges on responding to sexting incidents; …

- Although viewed by many young people as 'normal' or 'flirting', by sending an explicit image, someone under 18 may technically be producing and distributing indecent images. They risk being prosecuted, even if the picture is taken and shared with their permission and can be at increased risk of blackmail, bullying, emotional distress and unwanted attention from sex offenders. Whilst it is usually more common with teenagers, this behaviour can impact on younger children, for example risk taking behaviour or natural curiosity; all settings therefore must consider how to respond
- DSLs should access the follow the UKCCIS sexting guidance for schools and colleges and use professional judgement when responding to sexting concerns.
  - 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 and KSCB have published sexting guidance for professionals.

- Other useful links:
  - UK Safer Internet Centre
  - Childnet – Sexting and the Law
  - Childnet – "Picture this" resource
  - SWGfL – "So you got naked online" booklet
  - Think U Know 14+
  - Think U Know 11-13
  - NSPCC -Share Aware Resources
  - ChildLine – Zipit app
  - NSPCC

Children with special educational needs and disabilities (p26)

102. Children with special educational needs (SEN) and disabilities can face additional safeguarding challenges. Governing bodies and proprietors **should** ensure their child protection policy reflects the fact that additional barriers can exist when recognising abuse and neglect in this group of children. These can include:
    - assumptions that indicators of possible abuse such as behaviour, mood and injury relate to the child's disability without further exploration;
    - being more prone to peer group isolation than other children;
    - the potential for children with SEN and disabilities being disproportionally impacted by behaviours such as bullying, without outwardly showing any signs; and
    - communication barriers and difficulties in overcoming these barriers.

    To address these additional challenges, schools and colleges **should** consider extra pastoral support for children with SEN and disabilities.

- Settings should be mindful that the internet can both support children with SEND, as well as exacerbate any vulnerabilities. Guidance regarding online safety and SEND can be found on Kelsi.

Action points:
- What steps has the setting taken to implement additional online safety education and support to children with SEND?

Part 5: Child on child sexual violence and sexual harassment (p62-74)

236. 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 sexual violence and sexual harassment guidance clearly identifies that this behaviour can take place both on and offline.

- Childnet's project deSHAME provides useful information for educational settings regarding online sexual violence and harassment.

242. …where the report includes an online element, being aware of searching screening and confiscation advice (for schools) and UKCCIS 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 UKCCIS guidance and ensure staff are aware of how to respond to concerns.
    - Paragraph 250 also recognises the role of the Internet Watch Foundation as a possible point of support for seeking the removal of indecent images.

Annex A: Further information (p75-87)

Annex A contains important additional information about specific forms of abuse and safeguarding issues. School and college leaders and those staff who work directly with children **should** read this annex.

Child sexual exploitation (p76-77)

- 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. CSE can also take place completely online, for example children being coerced into performing sexual acts via webcam; it may not always result in a physical meeting between children and the offender.
    - 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 KSCB.

Action points:

- Does the child protection policy include responding to the use of technology as a tool for CSE?
- Are the specific factors regarding the use of technology within CSE (such as exploitation via live streaming) covered within staff training?

Child criminal exploitation: county lines (p77-78)

- Although not specifically mentioned, the internet can play a role in gang activity, such as gifts of technology and communication and intimidation over social media.

Preventing radicalisation (p81-83)

- This section highlights the role of the internet as a tool in the radicalisation of young people and in the potential accidental and deliberate exposure of young people and adults to extremism views and content online. DSLs should be aware of national and local policy and procedures regarding responding to concerns relating to 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 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.

Action points:

- Does the child protection policy include the use of technology as a tool for radicalisation?
- Has the DSL and staff had appropriate training regarding radicalisation and Prevent?
- How are children educated to be aware of radicalisation (including online) appropriately to their age and ability?

Peer on peer abuse and Sexual violence and sexual harassment between children in schools and colleges (p83-86)

- 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

- This section highlights the role of technology within peer on peer abuse (cyberbullying) and examples of online sexual harassment for staff.

Annex B: Role of the designated safeguarding lead

This section (p88-91) 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 may also apply to online safety concerns, especially as some issues will require referral to other agencies. Settings should raise awareness of recognising, responding, recording and referring online safeguarding issues 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).
- 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…
- The DSL is specifically identified as having the lead responsibility for online safety.
- DSLs should access appropriate online safety training to ensure they are aware of the specific online concerns 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 e-Bulletin, the Education Safeguarding Team's Child Protection Newsletter, the online safety pages on Kelsi, the Kent online safety Twitter feed and the Kent Online Safety blog accessed via the Education People website. DSLs are also able to access specific online safety consultations via the Kent Education Safeguarding Team.
    - Specific guidance regarding online safety and SEND can also be accessed on Kelsi.

Action points:

- Has the DSL accessed appropriate training regarding online safety?
    - Does this training include developing an up-to-date awareness of both the risks and benefits of technology?
    - Does it provide an awareness of both national and local policy and procedures?
    - Does it explore issues relating to online safety and SEND?

Annex C: Online safety (p92-94)

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 as identified by the 3 C's; 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 by the 3 C's (not just "grooming" by strangers).

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

A selection of resources is listed to enable settings to consider online safety education.

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.

- 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 may wish to 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 schools and settings using the EIS 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 understand 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 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 make informed decisions regarding the school/college filtering and monitoring systems and associated decisions?
    - How is this evidenced?
- How is this information shared with the community? For example, is it explicitly covered within the online safety or child protection policy?
- How does the leadership team 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 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.

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 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 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 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 therefore essential.

- The Kent County Council online safety policy template and guidance has specific content for settings regarding appropriate filtering and monitoring and also regarding the use of personal devices and mobile phones.

Action points:

- Does the setting 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 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 policy regarding safe and appropriate use of mobile phones and personal devices?

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. UKCCIS have recently published Online safety in schools and colleges: Questions for the governing board

- Settings may also wish to use the Kent educational setting self-review tools available via Kelsi: www.kelsi.org.uk/child-protection-and-safeguarding/e-safety

Staff training

Governors and proprietors **should** ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 76) and the requirement to ensure children are taught about safeguarding, including online (paragraph 80), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach

- This identifies that all members of staff should have access to appropriate, regular and up-to-date online safety training as part of their safeguarding training. Settings should consider how this is implemented within their own settings, for example will it be integrated within existing safeguarding and child protection training or provided as separate and specific online safety training.
- Online safety training should be accessed by ALL members of staff, not just teaching staff. A child could disclose an online safety concern to any adult, therefore all members of staff should be made aware of how to recognise, respond to, record and referral all safeguarding concerns, including online issues. The setting leadership team should also access this 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 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
- KSCB – Safer Practice with Technology

Action points:

- How does the setting 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, leadership staff and volunteers?
- Does staff training cover professional practice issues as well as safeguarding children?

Information and support

- The guidance links to a range of places to help settings access additional support and resources.
  - 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 e-Bulletin, the Education Safeguarding Team's Child Protection Newsletter, the online safety pages on Kelsi, the Kent online safety Twitter feed and the Kent Online Safety blog accessed via the Education People website.
  - Kent educational settings can contact the Education safeguarding Adviser (Online Protection) and e-Safety Development Officer directly for advice, support and guidance regarding online safety.

Action points:

- How does the setting (especially 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 implemented from 3rd September 2018.

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