Rebecca Avery, Education Safeguarding Adviser (Online Protection)
Education Safeguarding Service, The Education People July 2019

'Keeping Children Safe in Education' 2019: Online Safety Content and Updates

On the 26th June 2019 the Department for Education (DfE) published the updated 'Keeping children safe in education' (KCSIE) guidance ready for implementation from the 2nd September 2019. Schools and Colleges must comply with KCSIE 2018 until that date. KCSIE is statutory guidance from the DfE; all schools and colleges must have regard to it when carrying out their duties to safeguard and promote the welfare of children.

This document focuses on elements of KCSIE 2019 relevant to **online safety** including additions and changes from KCSIE 2018. It is recommended that DSLs and leaders read the entire KCSIE 2019 document when evaluating their current safeguarding practice and considering required actions for September 2019.

Summary of key points and changes related to online safety in KCSIE 2019:

- DSLs have overall responsibility for online safety (Annex B) but are encouraged to work with other staff within the setting as appropriate.
- DSLs should be able to evidence that they have accessed appropriate training and/or support to ensure they are understand the unique risks associated with online safety, can recognise the additional risks that learners with SEN and disabilities (SEND) face online, and that they have the relevant knowledge and up to date capability required to keep children safe online.
- All staff should provide with online safety training at induction and as part of their regular child protection training and updates.
- Part 5 states that child on child sexual violence and sexual harassment can occur both on and offline; additional content has been included with regards to 'Upskirting'.
    - All staff should have an awareness of peer on peer abuse issues such as sexting, cyberbullying and upskirting and know how to respond to these concerns.
- Online safety should be taught to all learners as part of providing a broad and balanced curriculum including as part of the requirements for Relationships Education and Relationships and Sex Education.
- Additional links have been added to annex C, 'online safety'; including a link to new DfE non-statutory guidance regarding 'Teaching online safety in schools'.

How to read this document:

- This font indicates a direct quote from the KCSIE 2019 guidance.
- This font indicates content has been added or amended since KCSIE 2018.
- This font is used to highlight recommendations, good practice and useful links.
- This font indicates a possible action points for DSLs and leadership staff to consider in readiness for September 2019.

Note: The DfE use the terms "must" and "should" throughout the guidance; "must" is used when the person in question is legally required to do something and "should" when the advice set out should be followed unless there is good reason not to. Governing bodies, proprietors, academy trusts **must** ensure that all staff read at least part one of the guidance. They should also ensure that mechanisms are in place to assist staff to understand and discharge their role and responsibilities as set out in part one of the guidance.

Part one: Safeguarding information for all staff

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

2. Safeguarding and promoting the welfare of children is **everyone's** responsibility...
    - Safeguarding (which includes online safety), is identified as a responsibility for all members of educational settings communities.

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

13. **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 includes online safety.

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

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…
    - This includes online safety abuse and safeguarding issues.

Indicators of abuse and neglect (p8)

23. 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.
    - 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 your anti-bullying policy specifically include cyberbullying?
- Does your policy outline the procures to follow if cyberbullying concerns are reported?

24. Sexual abuse: …may include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse. Sexual abuse can take place online, and technology can be used to facilitate offline abuse…

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

Action points

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

26. 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.

27. 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)…; Upskirting which typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm; …sexting (also known as youth produced sexual imagery) …
    - All members of staff should be aware of range of safeguarding issues; this specifically includes staff being aware of cyberbullying, 'upskirting' and sexting.

28. 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 cyberbullying, upskirting and 'sexting' concerns appropriately.

32. 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 known as contextual safeguarding, which simply means assessments of children should consider whether wider environmental factors are present in a child's life that are a threat to their safety and/or welfare.
    - This is especially likely to be the case with regards to online safety concerns.

Action points:

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

Part two: The management of safeguarding

Legislation and the law (p17)

51. 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.

Action points:

- Do your governing body/proprietors have enough understanding of the relevant legislation and statutory obligations regarding online safety?

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.
        - Individual schools and colleges should have a specific and robust child protection policy which is updated at least annually and is publicly available. It is not a statutory requirement to have a separate online safety policy, however if settings do not adopt this approach, they should ensure key elements (such as filtering and monitoring, social media and use of mobile technology) are integrated into the child protection policy or other relevant safeguarding policies.
        - If possible, staff should be involved in the development and construction of online safety and acceptable use 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.
        - Kent provides an Online Safety Policy template (please note this is currently being updated for September 2019) 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

    - A staff behaviour policy (sometimes called the code of conduct) which should, amongst other things, include acceptable use of technologies, staff/pupil relationships and communications including the use of social media.
        - The staff behaviour policy should explicitly cover the settings expectations regarding professional conduct online. Settings should ensure all staff have read and understood the relevant policies and procedures; which should be reviewed (at least annually) and updated and shared with staff on a regular basis.
        - The Education People provide a template Acceptable Use Policy (AUP) and online safety policy template which can be used by schools and colleges to develop and support a staff behaviour policy.
        - Other useful links for template documents include:
            - South West Grid for Learning
            - London Grid for Learning

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.

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

Action points:

- Does your child protection policy include issues in relation to online safety; either within the child protection policy or as a separate policy?
    - Is it up-to-date?
    - Is it publicly available - do all members of the community know how to access it?
- Does your staff behaviour policy/code of conduct cover the acceptable use of technology for staff, online staff/pupil relationships and communication via social media?
    - How do you ensure that this information is communicated with and understood by all members of staff?
    - How do you evidence this?
- How do you share policy changes and updates with staff?

The designated safeguarding lead (p19)

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…

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…remains with the designated safeguarding lead. This responsibility should not be delegated.

    - The ultimate responsibility for online safety falls within the remit of the Designated Safeguarding Lead (DSL).
        - Staff with appropriate skills, interest and expertise regarding online safety (such as computing leads or technical staff) should be encouraged to help support the DSL as appropriate, for example when developing curriculum approaches or making technical decisions. However, settings should be clear that overall responsibility for online safety cannot be delegated and remains with the DSL.

Action points:

- Is the settings DSL the lead person responsible for online safety?
    - Is this made clear to all members of staff?
    - How does the setting evidence that the DSL has lead responsibility?
- Has the school identified other members of staff who have skills, expertise or interests who may be able to support the DSL?
    - If appropriate, have they had specific training to enable them to act as a deputy DSL?

Staff training (p23)

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

    - Child protection training should explicitly cover online safety as part of all staff members induction.

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

Action points:

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

Online safety (p.23)

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 settings should recognise the role of the internet within child protection concerns and ensure appropriate systems are in place to filter and monitor internet activity.
      - The UKCIS Education Group has developed guidance for school governors to help governing boards support their DSL to keep children safe online.

Action points:

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

Opportunities to teach safeguarding (p23)

88. 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.

89. This may include covering relevant issues through Relationships Education and Relationships and Sex Education (formerly known as Sex and Relationship Education), tutorials (in colleges) and/or where delivered, through Personal, Social, Health and Economic (PSHE) education. The Government has made regulations which will make the subjects of Relationships Education (for all primary pupils) and Relationships and Sex Education (for all secondary pupils) and Health Education (for all pupils in state-funded schools) mandatory from September 2020.

90. 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 school/college's curriculum.

  - The responsibility for teaching children about online safety is not the sole responsibility of the computing curriculum; it should also be explicitly taught within Relationships and Sex Education (RSE) and be woven throughout the curriculum for all age groups. One-off events, lessons or assemblies or a reliance on external speakers, 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 sole source of education or sanctions; in some cases, this approach can undermine settings ability to develop internal capacity to respond to concerns. UKCIS have published guidance for educational settings regarding the use of external visitors.
  - The online safety curriculum should be flexible, relevant and engage learners' interests, be appropriate to their own needs and abilities and encourage them to develop resilience to online risks.
  - Settings should ensure they use a range of relevant resources and be mindful that online safety educate content can date quickly due to the rapid pace of change within technology.
  - Good practice is to gain learner input into the online safety curriculum; this could involve use of learner councils or use of peer education approaches.
- The UKCIS 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.

Action points:

- How does your 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 your learners needs, ages and abilities?
- How does your 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 your setting use external speakers to complement internal education approaches?

Peer on peer abuse (p25-26)

97. **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.

98. 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;
    - 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 Internet Safety (UKCIS) 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 offenders. Whilst it is usually more common with teenagers, this behaviour can occur with younger children, for example risk taking behaviour or natural curiosity; all settings therefore must consider how to respond to concerns.
- DSLs should access the follow the UKCIS sexting guidance for schools and colleges and use professional judgement when responding to sexting concerns.
    - Links to national guidance and support regarding responding to sexting can be found within the Kent online safety policy template.
    - The local procedures also include responding to harmful behaviours and underage sexual activity and sexting guidance for professionals.

Action points:

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

Children with special educational needs and disabilities (p28)

110. 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 vulnerabilities.

Action points:

- What steps has the setting taken to implement additional online safety education and support to children with SEND and other additional vulnerabilities?

Part 5: Child on child sexual violence and sexual harassment (p65-77)

248. 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 national guidance clearly identifies that child on child sexual violence and sexual harassment behaviour can take place both on and offline.
    - Childnet's project deSHAME provides useful information for educational settings regarding online sexual violence and harassment.

254. …where the report includes an online element, being aware of searching screening and confiscation advice (for schools) and UKCIS sexting advice (for schools and colleges). The key consideration is for staff not to view or forward illegal images of a child. The highlighted advice provides more details on what to do when viewing an image is unavoidable.

- DSLs should access the UKCIS guidance and ensure that all staff are aware of how to respond to potential sexting concerns.
- Paragraph 262 also recognises the role of the Internet Watch Foundation as a possible point of support for seeking the removal of illegal images.

Annex A: Further information (p78-91)

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 (p79)

- 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 online safety policy template covers responding to online CSE concerns. Further information about local approaches is available on Kelsi.

Child criminal exploitation: county lines (p80)

- 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.

Domestic Abuse (p81)

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

Preventing radicalisation (p84)

- 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 child protection policy template and online safety policy template covers responding to concerns regarding radicalisation. Further information about Prevent Duty and the Kent approach (including procedures, tools and training) can be found on Kelsi .
    - The Department for Education has published advice for settings on the Prevent duty. The Government has also launched a website called 'Educate Against Hate', which is designed to equip school and college leaders, teachers and parents with the information, tools and resources they need to recognise and address extremism and radicalisation in young people and this includes online issues.

Peer on peer abuse and sexual violence and sexual harassment between children in schools and colleges (p88)

- Whilst not intended to be an exhaustive list, sexual harassment can include:
    - Online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. It may include:
        - non-consensual sharing of sexual images and videos;
        - sexualised online bullying;
        - unwanted sexual comments and messages, including, on social media; and
        - sexual exploitation; coercion and threats
        - Upskirting
- Upskirting
    - 'Upskirting' typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm. It is now a criminal offence.
- This section highlights the role of technology within peer on peer abuse and provides examples of online sexual harassment.

Action points:

- Does your child protection policy include the use of technology as a tool within specific forms of abuse identified in annex A?
    - Have the DSL and staff had appropriate training?
    - How are children educated to be aware of the issues identified in annex A appropriately to their age and ability?

Annex B: Role of the designated safeguarding lead (p92)

This section (p91-95) highlights the roles and responsibilities of the DSL(s) including managing referrals, working with others, training, record keeping, awareness raising and availability; this will apply to online safety concerns. Settings should raise awareness of recognising, responding, recording and referring online safeguarding issues in line with the child protection policies and procedures with all members of staff.

Online safety is explicitly mentioned in the following contexts:

- The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection (including online safety). This should be explicit in the role holder's job description. This person should have the appropriate status and authority within the school to carry out the duties of the post. They should be given time, funding, training, resources and support to provide advice and support to other staff on child welfare and child protection matters, to take part in strategy and inter-agency meetings, and/or to support other staff to do so, and to contribute to the assessment of children.

- Work with others
    - The designated safeguarding lead is expected to…liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOS …) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies;
        - Whilst the DSL holds lead responsibility for online safety, they should work with other staff as necessary.

Action points:

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

- Training:
    - In addition to the formal training …, their knowledge and skills should be refreshed (this might be via e-bulletins, meeting other designated safeguarding leads, or simply taking time to read and digest safeguarding developments) at regular intervals, as required, and at least annually, to allow them to understand and keep up with any developments relevant to their role so they:
        - are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college;
        - can recognise the additional risks that children with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online…
    - DSLs should access appropriate online safety support and training to ensure they are aware of the specific online concerns that children, young people and adults may encounter. They should be able to evidence that they 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 Education Safeguarding Team's Child Protection Newsletter, Kent Online Safety Twitter feed and the Education People Blog. Kent DSLs are also able to access specific online safety consultations via the Education Safeguarding Service.

Action points:

- Has the DSL accessed appropriate training and support regarding online safety?

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

Annex C: Online safety (p96-99)

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. The 2019 edition has been updated to refer to new DfE guidance ' Teaching online safety in school' which outlines how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.

Action points:

- Have appropriate staff (subject leads, class teachers etc.) read and implemented the 'Teaching online safety in school' guidance in accordance to your setting's specific needs?
    - How can you evidence this?

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 made informed decisions regarding the school/college filtering and monitoring systems and associated decisions?
    - How is this evidenced?
- How is this information shared with the community? For example, are the settings approaches to appropriate filtering and monitoring explicitly covered within the online safety and/or child protection policy?

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

Action points:

- How do all members of staff ensure that technology in the classroom is used as safely and effectively?
    - Does the setting provide all members of staff with clear expectations regarding use of technology e.g. supervision, pre-checking content before use, use of age appropriate tools, understanding of data protection concerns, clear risk assessments etc.
- Does the setting have a clear policy regarding safe and appropriate use of mobile technology, including phones and other personal devices?
    - How is this communicated to staff, pupils and parents/carers?

Reviewing online safety

Technology in this area evolves and changes rapidly. A free online safety self-review tool for schools can be found via the 360 safe website. UKCIS have recently published Online safety in schools and colleges: Questions for the governing board.

- Settings may also wish to use the Kent tools available via Kelsi.

Action points:

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

Staff training

Governors and proprietors **should** ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 84) and the requirement to ensure children are taught about safeguarding, including online (paragraph 87), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

- All members of staff should have access to appropriate, regular and up-to-date online safety information as part of their safeguarding training. Settings should consider how this is implemented, for example, will it be integrated within existing safeguarding and child protection training or provided as separate and specific online safety inputs.
- Online safety training should be accessed by ALL members of staff, not just teaching staff. A child could disclose an online safety concern to any adult; all members of staff should be made aware of how to recognise, respond to, record and refer online safety concerns. The setting leadership team should also access 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 Online Safety Development Officer who provide centralised training, consultations and support for DSLs and bespoke whole 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?
- 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 Online Safety Development Officer are located within the Education Safeguarding Service within the Education People. They provide schools and colleges in Kent with advice, guidance and training regarding online safety.
    - Local information about online safety is provided for DSLs through the Education Safeguarding Team's Child Protection Newsletter, Kent Online Safety Twitter feed and the Education People Blog.

Action points:

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

Summary

The online safety agenda has continually evolved over recent years; it is essential that DSLs, governing bodies and proprietors are able to evidence that they recognise the role of online safety within their statutory safeguarding responsibilities towards all members of the community.

Schools and colleges should review their current online safety practice and consider changes required to be implemented from 2nd September 2019.

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