Making sense of…

Keeping Children Safe in Education 2016

➢ Online Safety guidance for Schools and Colleges

Keeping children safe in education

Statutory guidance for schools and colleges

September 2016

Online Safeguarding – Keeping Children Safe in Education 2016

Introduction

The 2016 revisions to the DfE statutory guidance Keeping Children Safe in Education (KCSIE) sees a number of significant changes. The revised guidance includes a welcome emphasis on Online Safety for Schools and Colleges, highlighted across numerous related sections. In response to enquiries received, this guidance has therefore been compiled to support Schools and Colleges in addressing the online aspects of the revised statutory guidance and whilst not intended to be exhaustive, seeks to highlight the considerable number of sections which include an online safety-related focus along with supporting advice and resources.

Lancashire Safeguarding Children Board: September 2016

Layout Key:

Highlighted extracts from Keeping Children Safe in Education 2016

LSCB guidance relating to extracts identified

Recommended advice and resources to support progression

ⓘ KCSIE Page 11; para 35-36 ▾

Types of abuse and neglect

35. **All school and college staff should be aware that abuse, neglect and safeguarding issues are rarely standalone events that can be covered by one definition or label. In most cases multiple issues will overlap with one another.**

36. **Abuse:** a form of maltreatment of a child. Somebody may abuse or neglect a child by inflicting harm or by failing to act to prevent harm. Children may be abused in a family or in an institutional or community setting by those known to them or, more rarely, by others (e.g. via the internet). They may be abused by an adult or adults or another child or children.

Lancashire Safeguarding Children Board

ⓘ KCSIE Page 11; para 38 ▾

> 38. **Emotional abuse**: the persistent emotional maltreatment of a child such as to cause severe and adverse effects on the child's emotional development […] It may involve seeing or hearing the ill-treatment of another. It may involve serious bullying (including cyberbullying) […]

This clearly identifies that online or 'cyber' bullying can result in emotional abuse. Schools and Colleges must therefore ensure that their Anti-Bullying Policies are up-to-date and include reference to their approach to dealing with all forms of bullying, including online.

Preventing and tackling bullying
Advice for headteachers, staff and governing bodies

DfE > Preventing and tackling bullying – Advice for schools
www.gov.uk/government/publications/preventing-and-tackling-bullying

Childnet > Education guidance to support tackling online bullying
www.childnet.com/teachers-and-professionals/for-working-with-young-people/hot-topics/cyberbullying

ⓘ KCSIE Page 11; para 39 ▾

> 39. **Sexual abuse**: involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving a high level of violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing and touching outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse (including via the internet). Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children.

This highlights that sexual abuse can occur via the Internet and can involve a range of activities, including (but not limited to) online grooming and exploitation, exposure to pornographic content and engaging a child in sexual activity online. This also identifies that perpetrators can be male or female and may include children themselves (such as in cases of Sexting). This clearly identifies that **Schools and Colleges must include the online aspects when addressing Child Sexual Exploitation (CSE)** and therefore must ensure that Safeguarding and Child Protection policies and procedures cover online sexual abuse.

ⓘ KCSIE Page 12; para 41-42

Specific safeguarding issues

41. **All** staff should have an awareness of safeguarding issues- some of which are listed below. Staff should be aware that behaviours linked to the likes of drug taking, alcohol abuse, truanting and sexting put children in danger.

All members of staff must be aware of a range of safeguarding issues, and specifically highlights the need for staff to be aware of Sexting. Sexting can be defined as 'an increasingly common activity among children and young people, where they share inappropriate or explicit images online…'. This can include sharing indecent images of themselves or others via mobile phones, webcams, social media and instant messaging.

*Although viewed by many young people as a 'normal' or 'mundane' activity and part of 'flirting', by sending an explicit image, a young person is producing and distributing child abuse images and risks being prosecuted, **even if the picture is taken and shared with their permission**. They can also be at increased risk of blackmail, bullying, emotional distress and unwanted attention. Whilst it is usually more common with teenagers, sexting behaviour can impact on younger children, for example risk taking behaviour or natural curiosity so all schools must consider how to respond.* (NSPCC)

NSPCC
Sexting
How to talk to children about the risks of sexting - and what you can do to protect them

NSPCC > The risks of Sexting
How to talk to children about the risks of Sexting
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting

Sexting is an issue which can be highlighted within staff safeguarding training. **DSLs should also take action to ensure that all members of staff are explicitly clear on how to respond to Sexting concerns appropriately and in line with the school/college policy.** For example, are all members of staff aware that if a child discloses they have sent or received a "sext" or "nude selfie", then these images should not be printed, copied or forwarded. The UK Safer Internet Centre have produced some very useful summary guidance on appropriately responding to and managing Sexting incidents. The UK Council for Child Internet Safety (UKCCIS) have also recently (August 2016) published comprehensive guidance and supporting resources for schools and colleges responding to Sexting incidents:

Advice for schools:
Responding & Managing to Sexting Incidents
Context
For School Staff
For the Designated Safeguarding Lead

UKSIC > Responding to and Managing Sexting Incidents
Support resource for Schools and DSLs (May 2016)
http://swgfl.org.uk/magazine/Managing-Sexting-Incidents

Sexting in schools and colleges: responding to incidents and safeguarding young people
UKCCIS
UK COUNCIL FOR CHILD INTERNET SAFETY
August 2016

UKCCIS > Sexting in schools and colleges:
Responding to incidents and safeguarding young people (August 2016)
https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

Whilst we will naturally have a preventative approach towards Sexting, post-incident advice to support young people experiencing issues resulting from Sexting is important. The South West Grid for Learning (SWGfL) have produced a useful (freely available) resource which provides practical advice and information for Young People experiencing issues:

SWGfL > So you got naked online…
www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/teaching-internet-safety/resources/sexting

42. **All** staff should be aware safeguarding issues can manifest themselves via peer on peer abuse. This is most likely to include, but not limited to: bullying (including cyber bullying), gender based violence/sexual assaults and sexting. Staff should be clear as to the school or college's policy and procedures with regards to peer on peer abuse.

This highlights that ALL members of staff must be advised that abuse can also be perpetrated by Children and Young People themselves and again, specifically highlights cyberbullying (Online Bullying) and Sexting. **Training should ensure that all members of staff are aware that not all online abuse is committed by adults or strangers and the education provided to children should reflect this**.

ⓘ KCSIE Page 12-13; para 43-44 ▾

43. Expert and professional organisations are best placed to provide up-to-date guidance and practical support on specific safeguarding issues. […]:

- bullying including cyberbullying
- child sexual exploitation (CSE) – and Annex A
- preventing radicalisation – and Annex A
- sexting

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

This highlights specific forms of abuse. In this context, it is apparent that each of these has related online aspects that should be considered when addressing Online Safety within school. Annex A specifically highlights forms of abuse which may involve the internet, including Child Sexual Exploitation (CSE) and Radicalisation.

ⓘ KCSIE Page 14; paras 47-48 ▾

Part two: The management of safeguarding

The responsibility of governing bodies, proprietors and management committees

> **Safeguarding policies**
> 47. Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare.
>
> 48. This should include:
>
> • an effective child protection policy; and
>
> • a staff behaviour policy (sometimes called the code of conduct) which should amongst other things include - acceptable use of technologies, staff/pupil relationships and communications including the use of social media.[12]

The emphasis on the responsibilities of Governing bodies/proprietors is explicitly evident throughout KCSIE. Understanding the potential risks and how these are being addressed should be clearly understood. Whilst all Governors should receive training, **typically the Governor with responsibility for child protection will receive more in-depth information and involvement**.

Note: Further to regularly queries, a locally-developed summary checklist resource is under development to support Governors as part of their approach to addressing Online Safety provision. This resource will be made available via the Online Safeguarding section of the LSCB website (www.lancashiresafeguarding.org.uk/online-safeguarding.aspx) once available.

This section also highlights the need for schools and colleges to have robust safeguarding policies, including a staff behaviour policy, which covers the school's expectations and approaches towards online safety and professional online practice - **expectations on appropriate staff use of Social Media should clearly identified**. This will include child protection and safeguarding policies and the staff behaviour policy/code of conduct.

All members of staff will need to have read and understood the relevant online safety policies and procedures, and we would recommend that this is provided to all members of staff (including volunteers) as part of induction and that these policies are updated and shared with staff on a regular (at least annual) basis.

SWGfL colleagues have a highly recommended, wide range of freely-available Online Safety template policies and related appendices (including Codes of Conduct & Social Media) which can be adapted to suit local requirements. It is **strongly recommended Schools and Colleges review these templates** when developing their policies along with **utilising the award-winning 360° Safe Self Review tool** to review provision.

SWGfL > Online Safety Template Policies

Excellent range of Online Safety Policy templates for Schools

http://swgfl.org.uk/products-services/esafety/resources/online-safety-policy-templates

SWGfL > 360º Safe Online Safety Self Review Tool

Highly Recommended (freely available) Self Review Tool for Schools

https://360safe.org.uk/

ⓘ KCSIE Page 15; para 52 ▾

The designated safeguarding lead

52. Governing bodies and proprietors should appoint an appropriate **senior member** of staff, from the school or college **leadership team**, to the role of designated safeguarding lead. The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection. This should be explicit in the role-holder's job description (see Annex B which describes the broad areas of responsibility and activities related to the role).

Online Safety is primarily a Safeguarding (rather than ICT) issue and therefore, the responsibility for Online Safety falls within the remit of the Designated Safeguarding Lead (DSL). Some Schools and Colleges may choose to delegate some aspects of the activities regarding Online Safety to other members of staff (e.g. where there is specific curriculum or technical knowledge/expertise required). However, as Online Safety is clearly identified as a Safeguarding priority, it is not appropriate for the Online Safety lead to be another member of staff (e.g. Computing lead, ICT Coordinator or Network Manager), unless they have also completed the appropriate DSL training.

However, effectively addressing Online Safeguarding requires a collaborative, whole-school approach. Therefore, staff with appropriate skills, interest and expertise should be encouraged to help support the DSL(s) as appropriate, for example when developing curriculum approaches or making technical decisions. However, **Schools and Colleges must be clear that the responsibility for Online Safety rests with the Designated Safeguarding Lead** as a Safeguarding issue.

It is important that DSLs access appropriate and regular Online Safety training to ensure they are aware of the specific online concerns which children, young people and adults may encounter and are able to take appropriate steps to ensure that practice in their settings is in line with national and local policy and procedures.

ⓘ KCSIE Page 17; para 64-66 ▾

> **Staff training**
>
> 64. Governing bodies and proprietors should ensure that all staff members undergo safeguarding and child protection training at induction. The training should be regularly updated. Induction and training should be in line with advice from the LSCB.
>
> 65. In addition all staff members should receive regular safeguarding and child protection updates (for example, via email, e-bulletins, staff meetings), as required, but at least annually, to provide them with relevant skills and knowledge to safeguard children effectively.
>
> 66. Governing bodies and proprietors should recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns on a daily basis. Opportunity should therefore be provided for staff to contribute to and shape safeguarding arrangements and child protection policy.

Research regularly informs us that **staff training for schools is typically the weakest area of provision when addressing Online Safety**. Safeguarding and child protection training provided to staff, on induction (and at least annually), should include Online Safety. This is highlighted further in Annex C – Online Safety.

Good practice examples include Schools and colleges incorporating elements of Online Safety within existing safeguarding and child protection training as well as providing separate and specific sessions. Additional good practice includes having Safeguarding (including Online Safety) as a standing item at all staff meetings and **identifying discrete Online Safety training when planning the annual staff training calendar**.

Staff should be involved in the development of the Online Safety Policy and related procedures to promote ownership and understanding. This may involve including staff in development via discussions at staff meetings or reviewing policies with staff working groups. Additionally, **it is good practice to ensure pupils/students are also engaged to ensure the broader School/College provision appropriately reflects those areas of Online Safety that may be of concern**.

Lancashire Safeguarding Children Board in partnership with UKSIC colleagues provide a free-of-charge update through the highly-popular annual Online Safety Live Briefings held each year in January. Whilst it does not replace the requirement for formal Online Safety CPD training, it provides a useful short, sharp (2-hour) update on current aspects and trends around Online Safety for the Children's workforce and **DSLs are strongly recommended to attend wherever possible**.

LSCB > Annual Online Safety Live Briefings

Annual 2-hour Online Safety briefing session (free-of-charge)

See the LSCB website for current details:

www.lancashiresafeguarding.org.uk/online-safeguarding.aspx

ⓘ KCSIE Page 17; para 67 ▾

Online safety

67. As schools and colleges increasingly work online it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place. Additional information to support governing bodies and proprietors is provided in Annex C.

Emphasis on **the responsibilities of Governing bodies/Proprietors is again apparent** and this re-iterates that Online Safety is viewed as part of schools and college's safeguarding responsibilities. Schools and Colleges should therefore ensure the increasing role of the online environment within Safeguarding provision is evident and clearly reflected within and across related policies. Supporting tools and systems such as internet content filters and monitoring systems should be in place. **It is important to recognise that these are supporting tools and not a solution and therefore should be implemented to support and complement effective classroom practice and appropriate pupil/student behaviour as part of a wider holistic approach to managing internet access.**

The revised guidance has seen the addition of a dedicated Annex (Annex C) for Online Safety. **This is indicative both of the importance placed on ensuring Online Safety is appropriately addressed and, that Online Safety is firmly identified as a Safeguarding issue**.

ⓘ KCSIE Page 18; para 68-69 ▾

Opportunities to teach safeguarding

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

It is made clear that **Governing bodies and proprietors should ensure that Online Safety is specifically covered within the curriculum**. The responsibility for teaching children about staying safe online is clearly identified and should be embedded throughout the curriculum rather than limited to the Computing aspects. Online Safety education should start within early years and be developed and across all age groups. **Particular attention should be**

paid to KS2/KS3 transition as children become increasingly exposed to mobile technologies and Social Media platforms.

One-off events, lessons or assemblies regarding Online Safety or an over-reliance on external speakers to educate children will not be effective or adequate practice. External speakers can bring useful in-depth/specific expertise and provide a catalyst to a discussion or reinforce learning but should not be the sole source of education for children. **Developing the school's capacity to embed online aspects through PSHE and SRE should be a key aspect** and will support a longer-term approach, including building resilience and the capacity to respond to concerns as they arise.

Effective **Online Safety education should be embedded across the curriculum**, including through PSHE and Computing lessons and it is therefore good practice for staff to identify opportunities and reference ways in which the online aspects of Safeguarding can be reinforced in their respective lesson planning and delivery (e.g. when different subject areas utilise technology as teaching and learning tools).

Equally, Online Safety should also be taught discretely and provides the opportunity to encompass specific aspects the school may encounter or address concerns students may have raised.

Developing **Digital Literacy remains a key aspect in supporting Children and Young People and building their resilience to online issues**, both in recognising potential risks and developing their own online behaviour.

PSHE Association > Key principles of effective prevention education

Report on good practice produced on behalf of CEOP (April 2016)

www.pshe-association.org.uk/curriculum-and-resources/resources/key-principles-effective-prevention-education

SWGfL colleagues in partnership with Common Sense Media have developed an excellent range of practical resources covering a wide range of Online Safety topics from Foundation Stage through to KS4/5.

SWGfL > Digital Literacy & Citizenship Resources

Highly Recommended (freely-available) classroom resources

www.digital-literacy.org.uk

Highly Recommended

The school/college Online Safety curriculum should be flexible, relevant and engage pupils' interests, be appropriate to their own needs and abilities and encourage pupils to develop resilience to online risks. Schools and colleges should ensure they use a range of relevant resources and be mindful that Online Safety education content can often date very quickly due to the rapid pace of change within technology.

Good practice typically involves Schools and Colleges **ensuring learners have an input into developing the Online Safety curriculum**, helping to ensure it is current, relevant and their concerns are being covered. This may involve engaging with pupil/student councils or include elements of peer education.

Childnet > Practitioner Resource Bank
Resources, lesson plans and activities for children aged 3 - 19
www.childnet.com/resources

Highly Recommended

CEOP > ThinkUKnow (TUK) Teacher Resources
TUK Teacher Resource area
https://www.thinkuknow.co.uk/teachers/resources/

UKSIC > Teaching Internet Safety
Resource area including planning advice and resources
www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/teaching-internet-safety

> 69. Whilst it is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place; they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding

Governing bodies and proprietors should make informed decisions regarding filtering and monitoring systems and ensure decisions are appropriate to the school's technology provision as well as the needs of the learners. **A reliance on filtering to safeguard children is not appropriate** and children will need to be taught critical thinking skills which are appropriate to their age and ability.

Content filtering tools have become increasingly sophisticated and therefore a one-size-fits-all approach to content filtering across the whole school is neither recommended nor appropriate. Whilst there is naturally a need to ensure learners remain safe, content filtering systems now typically have facilities to allow schools to individually **customise filtering policies according to local requirements** and will help to avoid 'over-blocking'.

However, whilst increasingly sophisticated, it is essential that Schools and Colleges understand that **filtering and monitoring systems are NOT A SOLUTION** and must therefore be utilised to complement and support effective teaching and learning practices. Schools and Colleges may wish to consider developing a risk assessment approach or other process to **ensure filtering decisions are informed by and encompass Safeguarding, Technical and Educational priorities**.

Note: Further information and suggested resources around filtering and monitoring are included under Annex C below.

ⓘ KCSIE Page 18; para 70 ▾

Inspection

70. From September 2015 all inspections by Ofsted have been made under: A new common inspection framework: education, skills and early years. Inspectors will always report on whether or not arrangements for safeguarding children and learners are effective. Ofsted has published a document setting out the approach inspectors should take to inspecting safeguarding: Inspecting safeguarding in early years, education and skills settings. Individual inspectorates will also report on safeguarding arrangements and have published frameworks which inform how they inspect the independent schools that are not inspected by Ofsted at: School Inspection Service and Independent Schools Inspectorate.

The **Ofsted 'Inspecting safeguarding in early years, education and skills settings'** document was published in **August 2016** and regularly refers to Online Safety throughout the guidance for inspectors.

Ofsted

Inspecting safeguarding in early years, education and skills settings

Ofsted > Inspecting safeguarding in early years, education and skills settings (August 2016)

Safeguarding guidance for Ofsted inspectors

https://www.gov.uk/government/publications/inspecting-safeguarding-in-early-years-education-and-skills-from-september-2015

Schools and Colleges may wish to **audit current practice to identify strengths and areas for improvement**. A very highly recommended tool to support schools/colleges with this is the SWGfL 360° Safe self-review tool highlighted previously on page 6 of this guidance.

KCSIE Page 19; para 76-77

Allegations of abuse made against other children

76. Staff should recognise that children are capable of abusing their peers. Governing bodies and proprietors should ensure their child protection policy includes procedures to minimise the risk of peer on peer abuse and sets out how allegations of peer on peer abuse will be investigated and dealt with. The policy should reflect the different forms peer on peer abuse can take, make clear that abuse is abuse and should never be tolerated or passed off as "banter" or "part of growing up". It should be clear as to how victims of peer on peer abuse will be supported.

77. Peer on peer abuse can manifest itself in many ways. Governors and proprietors should ensure sexting and the school or college's approach to it is reflected in the child protection policy. The department provides searching screening and confiscation advice for schools. The UK Council for Child Internet Safety (UKCCIS) Education Group has recently published sexting advice for schools and colleges.

This identifies that abuse can be perpetrated by children as 'peer-on-peer' abuse. It specifically highlights the need for governors and proprietors to ensure that School and College Safeguarding and Child Protection Policies include addressing and responding to peer-on-peer abuse, including Sexting. As part of their safeguarding responsibilities, **all staff should explicitly understand how to respond to and manage incidents appropriately in line with robust and clearly structured safeguarding procedures**.

DSLs in particular should ensure they are expressly familiar with local and national guidance and recommended good practice. The UKSIC and UKCCIS resources highlighted under 'Specific Safeguarding Issues' on page 3 above are excellent supporting resources to support Schools and Colleges with this aspect.

KCSIE Page 54; Annex A

Annex A: Further information

Further information on child sexual exploitation

(We expect to update this section in the summer when a updated definition of CSE has been agreed)

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

Child Sexual Exploitation (CSE) may involve utilising the Internet and Social Media to identify potential victims or as a tool to coerce and blackmail children into performing sexual acts, both on and offline. Means of accessing the Internet may also be provided to children as a "gift" by perpetrators such as in the form of new mobile phones and devices. In some cases, CSE can take place entirely online such as children being coerced into performing sexual acts via webcam/Social Media and therefore may not always result in a physical meeting between children and the offender. DSLs should be aware of National and Local policy and procedures regarding CSE and **ensure that policies and procedures relating to CSE explicitly include reference to online aspects**.

The Child Exploitation and Online Protection Centre (CEOP) through their ThinkUKnow (TUK) programme has a number of useful resources and media clips including the **'Exploited' CSE Prevention Resource** which can be used as a basis for specific learning activities in KS3/4+ classroom settings. In addition, the 'Click CEOP' Report button remains available to report concerns and can be added to websites and used as part of awareness raising activities.

CEOP > ThinkUKnow (TUK) 'Exploited' Resource

TUK CSE Prevention Resource

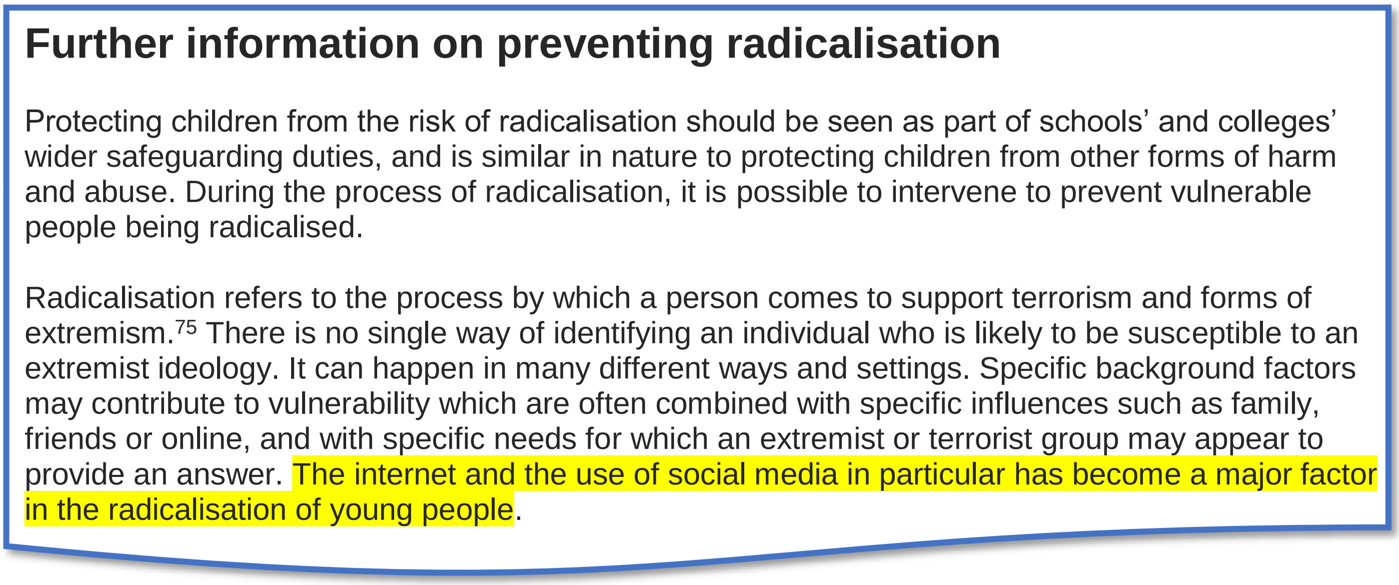
https://www.thinkuknow.co.uk/teachers/resources/

CEOP > Click CEOP Button

CEOP Safety Centre – Click CEOP

https://www.ceop.police.uk/safety-centre

ⓘ KCSIE Page 56-57; Annex A ▾



Further information on preventing radicalisation

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

Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism.[75] There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. It can happen in many different ways and settings. Specific background factors may contribute to vulnerability which are often combined with specific influences such as family, friends or online, and with specific needs for which an extremist or terrorist group may appear to provide an answer. The internet and the use of social media in particular has become a major factor in the radicalisation of young people.

This highlights the increased role of the **Internet and Social Media as tools used in the radicalisation of young people**. Understanding the similarities between Online Grooming and the Radicalisation often provides a useful perspective to address this area, particularly in relation to **ensuring C&YP are educated about Digital Literacy**. This section also highlights that procedures for responding to radicalisation may be set out in existing Safeguarding policies and separate 'Prevent' policies are not necessary.

DSLs should be familiar with the statutory requirements of the Government's Prevent Duty 2015 and particularly, the **DfE Departmental Advice for schools**. Policies and procedures should clearly encompass Radicalisation and Extremism highlighting both preventative activity and how issues will be managed / escalated (e.g. include escalation routes such as Channel where appropriate).

P4S > Useful information Section

Useful information section on preventforschools.org including local and national guidance such as the DfE Departmental Advice.

www.preventforschools.org/?category_id=55

Freely available **supporting resources** around the broader radicalisation/extremism agenda have recently been refreshed and **are available on the Lancashire preventforschools.org website**. This includes specific guidance produced for schools around **Online Radicalisation**.

P4S > Lancashire preventforschools.org website

Very popular Lancashire site providing access to a range of (freely available) classroom resources to address Prevent-related issues

www.preventforschools.org

Highly Recommended

P4S: ONLINE RADICALISATION

- guidance for Schools (Spring 2016)

P4S

P4S > Online Radicalisation

Useful information from the Lancashire P4S site around Online Radicalisation (March 2016)

www.preventforschools.org/?category_id=55

Trust me

Thinking critically about what you see online

Childnet International

Childnet > Trust Me (Thinking critically about what you see online)

Highly recommended Primary & Secondary resources to support building online resilience through Digital Literacy

www.childnet.com/resources/trust-me

Highly Recommended

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

> The Department for Education has also published advice for schools on the Prevent duty. The advice is intended to complement the Prevent guidance and signposts other sources of advice and support. The Government has launched educate against hate, a website 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. The website provides information on training resources for teachers, staff and school and college leaders, such as Prevent e-learning, via the Prevent Training catalogue.

Further information on appropriate filtering and monitoring systems is available from the UK Safer Internet Centre as highlighted in Annex C (Filtering & Monitoring) on pages 17-18 below.

An increasing number of filtering and monitoring system providers are engaging with the Provider Checklist for Appropriate Filtering / Appropriate Monitoring offered by the UK Safer Internet Centre. The checklist allows providers to illustrate how their particular product/s meet the national defined standards. It is **strongly recommended that Schools and Colleges should confirm with their service provider** whether the filtering and/or monitoring system provided has engaged in this scheme and if not, seek assurance that the product/s supplied implements ***"the police assessed list of unlawful terrorist content, produced on behalf of the Home Office".***

ⓘ KCSIE Page 62-63; Annex C ▾

Annex C: Online Safety

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

This clearly identifies Online Safety as a Safeguarding responsibility and highlights that an effective approach to Online Safety provides Schools and Colleges with the ability to educate all members of their communities **in their use of technology** and has systems and processes which allow timely intervention and escalation where appropriate.

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

- content: being exposed to illegal, inappropriate or harmful material
- contact: being subjected to harmful online interaction with other users
- conduct: personal online behaviour that increases the likelihood of, or causes, harm

This relates to the '3C's Risk Matrix' as originally identified through the LSE EU Kids Online project and is also referred to in the Pan-Lancashire LSCB Online Safeguarding Strategy as a means of categorising risk areas according to type. It is essential that Schools and Colleges therefore develop **a broad and balanced Online Safety curriculum** which covers a range of Online Safety risks across subject areas.

Pan-Lancashire LSCB
Online Safeguarding
Strategy
2017 - 2019

LSCB > Pan-Lancashire Online Safeguarding Strategy

Framework Strategy outlining the Pan-Lancashire approach to Online Safeguarding

www.lancashiresafeguarding.org.uk/online-safeguarding.aspx

Good practice typically demonstrates that **questioning pupils/students on their concerns helps to inform and ensure the curriculum is appropriate and meets the needs of learners**. In addition, Online Safety messages shared with staff and children should be appropriate and up-to-date and empower them to be able to respond to a range of online threats as well as opportunities. The previously mentioned SWGfL Digital Literacy & Citizenship resource referred to on page 9 is an excellent resource to support this aspect.

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.[81]
The UK Safer Internet Centre has published guidance as to what “appropriate” might look like:

- UK Safer Internet Centre: appropriate filtering and monitoring

Governing bodies and proprietors should ensure informed decisions are made regarding the safety and security of the internet access and equipment available in their settings. Governing bodies and proprietors must ensure that the welfare of children and young people is paramount at all times. Any decisions taken regarding filtering and monitoring systems should be taken from **a combined Safeguarding, Educational and Technical approach** and should be justifiable and documented. When reviewing filtering and monitoring systems, some governing bodies and proprietors may wish to undertake an approach which includes robust risk assessments and a thorough comparison which identify both the benefits and limitations of the services.

Schools may also wish to approach their provider/s to consider the range of tools available to them which may support and inform the development of strategies to manage and supervise Internet/system usage appropriately.

The UK Safer internet Centre have produced excellent guidance for Schools and Colleges about appropriate filtering and monitoring. It is **strongly recommended that governing bodies, proprietors and DSLs read and consider this guidance** when assessing their filtering and monitoring systems and any associated decisions.

UK Safer Internet Centre
Appropriate Filtering & Monitoring

UKSIC > Appropriate Filtering Guidance
Useful guidance for education settings about establishing appropriate levels of filtering
www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-and-monitoring/appropriate-filtering

Highly Recommended

UKSIC > Appropriate Monitoring Guidance

Useful guidance about establishing appropriate levels of monitoring

www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-and-monitoring/appropriate-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.

As highlighted previously, filtering and monitoring systems are NOT a solution. No system can offer schools and colleges 100% protection from exposure to inappropriate or illegal content, so it is equally important that establishments can demonstrate that they have taken all reasonable precautions to safeguard children and staff. Such methods may include (but are not limited to) appropriate supervision, requiring students and staff to sign (and support) Acceptable Use/Behaviour agreements, a robust and embedded Online Safety curriculum and appropriate and up-to-date staff training. An **over-reliance on filtering and monitoring to safeguard children online provides a false sense of security**, leading to complacency which may put children and adults at risk of significant harm both inside and outside of the school environment.

It is essential that all Governing bodies, proprietors and members of staff recognise that even with the most expensive and up-to-date security systems and filtering, children or staff can potentially bypass them either via using proxy sites or by using their own devices (e.g. smartphones or tablets) which would not be subject to the school/colleges filtering. **Online Safeguarding is fundamentally about Behaviours** rather than what technology is used Therefore, **evolving Acceptable Use Policies towards Acceptable Behaviour Policies** will support addressing access via personal devices using 3G and 4G connectivity by focusing on what is acceptable behaviour rather than what device is used and whether it is owned by the school or not.

Staff training

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

This identifies that all members of staff must have access to appropriate, regular and up-to-date Online Safety training as part of their Safeguarding provision. Schools and Colleges should consider how this is implemented within their own settings.

Research continues to inform us that **staff training is typically the weakest area of Online Safety in schools**. Given the continually evolving nature of Online Safety, it is strongly advised that ALL staff receive regular update training at least annually. Whilst they will each have a distinct focus, it is increasingly encouraged that this is **incorporated into planning for Parental Awareness Sessions** (e.g. Staff Session followed by Parental Session) to both ensure consistency and save costs.

During Online Safety Staff Sessions, some school leaders and non-teaching staff are absent due to demands on time, resources or other commitments. However, whilst ensuring a whole staff group presence is difficult, **Online Safety training should be accessed by ALL members of staff** (i.e. not limited to teaching staff). As a child could disclose an Online Safety concern to any adult, all members of staff (including external staff and volunteers) should be made aware of how to recognise, respond to, record and refer all safeguarding concerns, including online issues and Schools/Colleges should ensure mechanisms are in place to enable this to be achieved. It is also **important that School leaders also access this training** to ensure that messages are appropriate and consistent and to demonstrate to staff that this aspect of Safeguarding is a key priority at the School/College.

Further information, guidance and resources can be found via the LSCB website which includes a dedicated Online Safeguarding section for Lancashire-region colleagues and is regularly updated with news, events and information to support progression of the Online Safeguarding agenda.

The LSCB Online Safeguarding Adviser is located within the Lancashire LSCB/LSAB Team and provides Schools and Colleges with advice, guidance, support and training. Contact details for further enquiries are provided below.

Summary

As will be apparent, the Online Safeguarding agenda has evolved significantly over recent years and it is evident that Schools and Colleges (especially DSLs, Governing Bodies and Proprietors) have a crucial role in ensuring our Children and Young People are able to stay safe online and maximise the immense benefits technology brings. Equally, supporting our Children and Young People to stay safe online equips them with lifelong skills that will extend far beyond the academic environment and therefore it is immensely important that we provide them with the knowledge and skills to build resilience that will protect them against today's risks but also, those online challenges that may not yet be apparent. It is clear that this aspect of Safeguarding continues to evolve and develop and therefore cannot, and should not, be addressed as a task-and-finish issue.

This guidance, whilst not exhaustive, is intended to provide colleagues with support in addressing the varied online requirements of Keeping Children Safe in Education 2016 and seeks to highlight supporting resources and considerations in developing School and College Online Safety provision.

We hope you find this a useful, supportive and productive resource.

Graham Lowe
LSCB/LSAB Online Safeguarding Adviser
Chair, Pan-Lancashire LSCB Online Safeguarding Group

September 2016

E: graham.lowe2@lancashire.gov.uk
W: www.lancashiresafeguarding.org.uk

Concerns about a child should be reported on 0300 123 6720 or out of hours 0300 123 6722 (8pm - 8am)

Lancashire Safeguarding Children Board
Home
About Us
News
Resources
Learning & Development
Parents & Carers
CDOP
Online Safeguarding - An Introduction
Overview
Schools and the Children's Workforce
Teachers & Professionals
Information for Parents and Carers
Parents & Carers
Online Safeguarding News & Events
News & Events
Online Safety NEWS
Online Safeguarding - A Focus On...
Focus On...
Frequently Asked Questions (FAQs)
Frequently Asked Questions

Further advice and information about Online Safeguarding is available from the LSCB Online Safeguarding homepage at: www.lancashiresafeguarding.org.uk/online-safeguarding.aspx

Acknowledgements: This guidance has been produced to support schools and colleges in identifying and progressing the Online Safeguarding aspects of the revised DfE Keeping Children Safe in Education statutory guidance 2016. Advice has been referenced from a variety of colleagues and organisations and collates useful recommendations and good practice. However, particular recognition and our express gratitude should go to Rebecca Avery at Kent County Council.