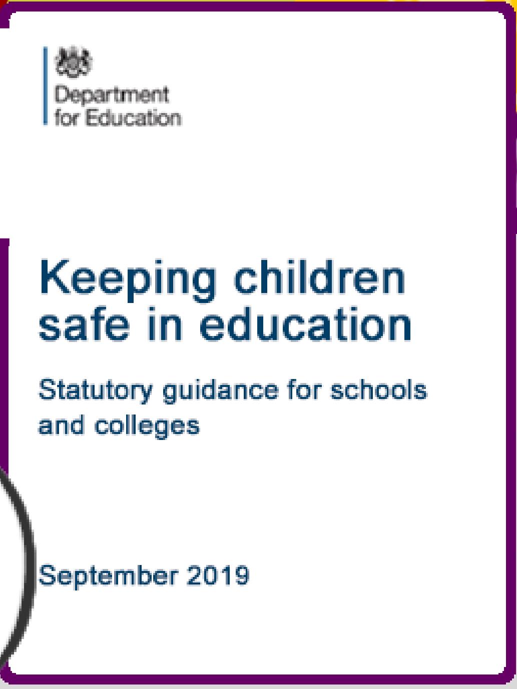
LSCB
3419

standards management access learning

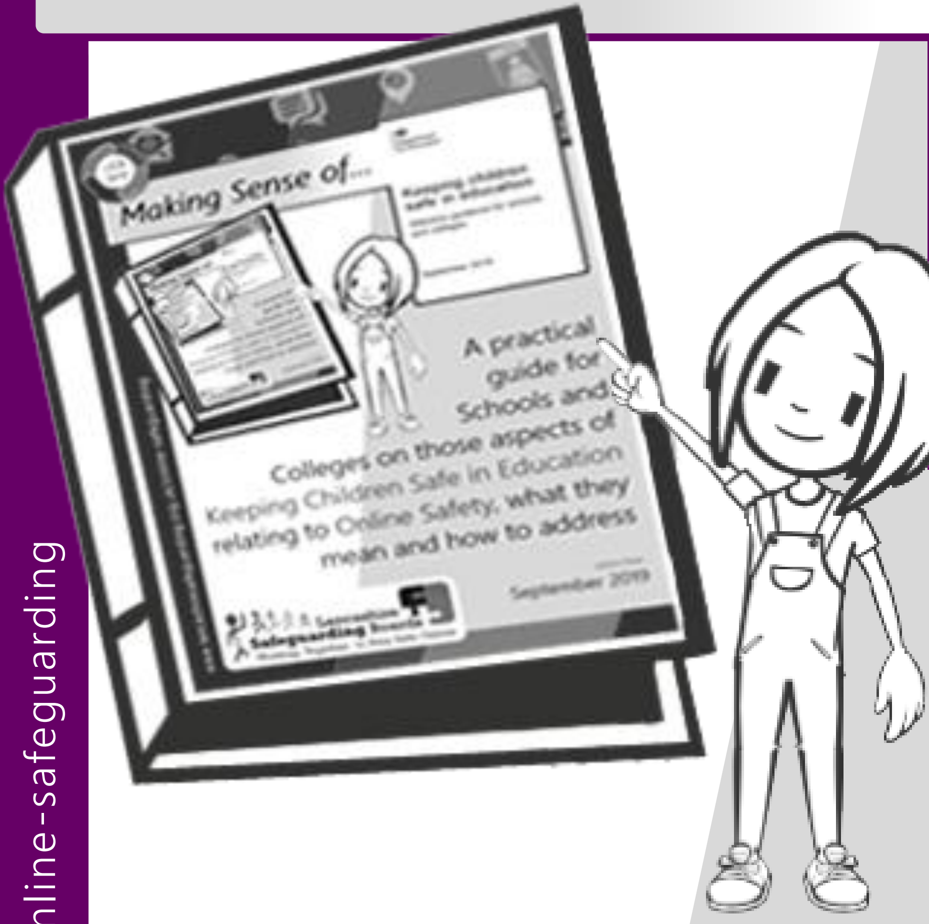
Making Sense of…


Department
for Education

Keeping children
safe in education

Statutory guidance for schools
and colleges

September 2019



A practical guide for Schools and Colleges on those aspects of Keeping Children Safe in Education relating to Online Safety, what they mean and how to address

: edition three :

September 2019

Lancashire
Safeguarding Boards
Working Together to Stay Safe Online

www.lancashiresafeguarding.org.uk/online-safeguarding www.lancashiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce#MakingSense

.: intentionally blank :.

Introduction

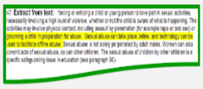
In 2016, further to requests from Headteacher and Designated Safeguarding Lead colleagues across the region, Lancashire Safeguarding Boards produced guidance for Schools and Colleges on those aspects that related to online safety within the newly-revised DfE Keeping Children Safe in Education (KCSIE) guidance. This explanatory guidance was further updated in 2018 and was highly-popular and extremely well-received. As a result, with the release of the 2019 revisions, the Safeguarding Board has once again reviewed the statutory guidance in order to extract, clarify and provide updated guidance on those relevant online safety-related areas as well as signposting recommended good-quality sources of support.

It continues to be apparent that the statutory guidance places significant emphasis on the importance of online safety and its place within effective safeguarding provision and whilst not intended to be exhaustive, the following resource again seeks to highlight both continued and new sections that will be of particular interest to Governors, School Leaders and Designated Safeguarding Leads.

Graham Lowe
Online Safeguarding Advisor
Chair, Pan-Lancashire Online Safeguarding Group
Lancashire Safeguarding Boards, September 2019

✉ graham.lowe2@lancashire.gov.uk
🏠 www.lancashiresafeguarding.org.uk

Layout Key: *Making Sense of...*KCSIE 2019

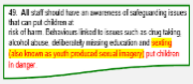


47. **Extract from text:** forcing or enticing a child or young person to take part in sexual activities, necessarily involving a high level of violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example rape or oral sex) or grooming a child in preparation for abuse. Sexual abuse can take place online, and technology can be used to facilitate offline abuse. Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children. The sexual abuse of children by other children is a specific safeguarding issue in education (see paragraph 50).

Highlighted extracts from Keeping Children Safe in Education 2019

Advice — LSCB advice and guidance relating to extracts identified

Resources — Recommended quality-assured resources to support progression



49. **All** staff should have an awareness of safeguarding issues that can put children at
risk of harm. Behaviours linked to issues such as drug taking, alcohol abuse, deliberately missing education and sexting (also known as youth produced sexual imagery) put children in danger.

RED text - new or re-worded information for KCSIE 2019

Abuse and neglect

20. 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.

21. **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. Abuse can take place wholly online, or technology may be used to facilitate offline abuse. They may be abused by an adult or adults or by another child or children.

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 seeing or hearing the ill-treatment of another. It may involve serious bullying (including cyberbullying) […]

Advice

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

Resources

Department for Education

Preventing and tackling bullying

Advice for headteachers, staff and governing bodies

July 2017

DfE > Preventing and tackling bullying – Advice for schools (July 2017)

DfE advice for Headteachers, staff and governing bodies

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

Advice

Online bullying is the most common concern highlighted by Children & Young People (C&YP) when discussing online safety. The highly-recommended Childnet resource 'Crossing the Line' referred to on page 15 of this guidance includes a theme of Cyberbullying as one of four aspects to support PSHE delivery around online challenges. The resource, "*Gone too far*" is aimed for use with 11-14s and includes teacher guidance, lesson plans, video, worksheets and a supporting powerpoint resource.

.

24. **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. Sexual abuse can take place online, and technology can be used to facilitate offline abuse. Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children. The sexual abuse of children by other children is a specific safeguarding issue in education (see paragraph 27).

Advice

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.

Specific safeguarding issues

26. **All** staff should have an awareness of safeguarding issues that can put children at risk of harm. Behaviours linked to issues such as drug taking, alcohol abuse, deliberately missing education and sexting (also known as youth produced sexual imagery) put children in danger.

Advice

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 is typically 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 often viewed by young people as a 'mundane' activity or 'normal flirtatious behaviour', by taking and sending an explicit image (even if the picture is taken/shared with their permission), a young person is producing and distributing an indecent image of a child and risks being prosecuted. This also increases the risk of bullying or blackmail and can be a significant source of emotional distress and unwanted attention. Sexting behaviour, although more commonly associated with teenagers, can also occur with younger children either through natural curiosity or as part of developing risk-taking behaviours and therefore all schools must consider carefully how they will respond.

Resources

NSPCC
EVERY CHILDHOOD IS WORTH FIGHTING FOR
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
www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting

Advice

Sexting is an issue which should 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*", then these images should not be printed, copied or forwarded? In those circumstances where further escalation is required (e.g. Police), this should be via the DSL. The UK Safer Internet Centre have produced some very useful summary guidance on appropriately responding to and managing Sexting incidents. The UK Council for Internet Safety (UKCIS (formerly UKCCIS)) has also published excellent comprehensive guidance and supporting resources for schools and colleges responding to Sexting incidents.

Note: It is strongly recommended that all DSLs should be expressly familiar with the UKCIS Sexting in schools and colleges guidance.

Additionally, in line with the UKCIS guidance, the LSCB has produced an A3 summary flowchart and FAQs resource which highlights recommend practice along with criteria for escalation and can be included within the School's Child Protection Policy.

Resources

UKCCIS
UK COUNCIL FOR CHILD INTERNET SAFETY
Sexting in Schools and Colleges:
Responding to incidents and safeguarding young people

Lancashire Safeguarding Boards
Very Highly Recommended

UKCIS > Sexting in schools and colleges (August 2016)
Responding to incidents and safeguarding young people
www.gov.uk/government/publications/sexting-in-schools-and-colleges

Responding to Sexting instances
LSCB
Process ☑ ☑ Reporting
Resources ☑ ☑ Support

LSCB > Responding to Sexting instances – flowchart:
Local flowchart & FAQs to support schools responding to instances
www.lancashiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce.aspx#SextingProcess

Advice for schools: Responding to & Managing Sexting Incidents
Context
For School Staff
Step 1
Step 2
For the Designated Safeguarding Lead

UKSIC > Responding to and Managing Sexting Incidents
Support resource for Schools and DSLs (May 2016)
https://swgfl.org.uk/resources/managing-sexting-incidents

Advice

Whilst we may understandably take a preventative approach towards Sexting, post-incident advice to support young people experiencing issues resulting from Sexting is essential. 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:

Resources

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

27. **All** staff should be aware that children can abuse other children (often referred to as peer on peer abuse). This is most likely to include, but may not be limited to:

- bullying (including cyberbullying);
- physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm;
- sexual violence,[8] such as rape, assault by penetration and sexual assault;
- sexual harassment,[9] such as sexual comments, remarks, jokes and online sexual harassment, which may be stand-alone or part of a broader pattern of abuse;
- upskirting,[10] 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); and
- initiation/hazing type violence and rituals.

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

Advice

This highlights that ALL members of staff should understand 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.

This section highlights specific forms of abuse. In this context, it is apparent that these points can include 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. The above extract also sees an additional factor in the 2019 update relating to '*Upskirting*' which is reflected on Page 25 of this guidance.

Part two: The management of safeguarding

The responsibility of governing bodies, proprietors and management committees

Safeguarding policies and procedures

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. The child protection policy should describe procedures which are in accordance with government guidance and refer to locally agreed multi-agency safeguarding arrangements put in place by the three safeguarding partners. It should be updated annually (as a minimum) and be available publicly either via the school or college website or by other means.
- 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.[20]

Advice

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. To support Governor colleagues, the LSCB has developed and updated a local summary checklist resource to aid colleagues as part of their approach to addressing online safety provision.

Resources

LSCB
Online Safety
Governance
Checklist
☑ Review
☐ Guidance
☐ for Governors
☑ & Proprietors

LSCB > Online Safety Governance Checklist: (updated August 2019)
Locally-developed Governor self-assessment checklist to support with reviewing school/college online safety provision
www.lancashiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce#GovernorSRT

UK Council for
Internet Safety

Online Safety in schools and colleges: Questions from the Governing Board

UKCIS > Governor Guidance:
Useful guidance from UKCIS in the form of 5 (overarching) questions Governing Boards should ask about Online Safety including what to look for; what is good practice and when there should be a concern
www.gov.uk/government/publications/online-safety-in-schools-and-colleges-questions-from-the-governing-board

Advice

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. It is recommended that this is provided to all members of staff (including volunteers) as part of induction and that these policies are reviewed and shared with staff on a regular (at least annual) basis.

A challenge often highlighted by colleagues when developing the School's/College's Online Safety policy is where to start from the wide array available. 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.

To aid in a robust, consistent and comprehensive approach, Lancashire Safeguarding Boards recommend Schools and Colleges make use of the excellent SWGfL templates when developing or reviewing Online Safety policies, along with utilising the award-winning 360° Safe Self Review tool to review and self-assess provision.

Resources

SWGfL > Online Safety Template Policies
Excellent range of Online Safety Policy templates for Schools
https://swgfl.org.uk/online-safety-policy-templates-for-schools/#download-documents

SWGfL > 360° Safe Online Safety Self Review Tool
Highly Recommended (freely available) Self Review Tool for Schools
https://360safe.org.uk/

The designated safeguarding lead

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

Advice

Online Safety is primarily a Safeguarding 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 (though not the responsibility*) of the activities regarding Online Safety to other members of staff (e.g. where there is specific curriculum or technical knowledge/expertise required).

* It is not appropriate for the lead responsibility to be given to 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 Safety 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 – typically achieved through the Online Safety Group. However, Schools and Colleges must be clear that the responsibility for Online Safety rests with the Designated Safeguarding Lead as a Safeguarding issue.

The designated safeguarding lead

66. The designated safeguarding lead and any deputies should undergo training to provide them with the knowledge and skills required to carry out the role. The training should be updated every two years.

67. In addition to their formal training as set out above, their knowledge and skills should be updated, (for example via e-bulletins, meeting other designated safeguarding leads, or taking time to read and digest safeguarding developments), at regular intervals, and at least annually, to keep up with any developments relevant to their role.

Advice

The online environment continues to develop at a pace and therefore, 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. This may include courses provided by external providers or those offered by the Local Safeguarding Partnership arrangements. Further information on this aspect is provided on pages 34 & 35 of this guidance.

Advice

Updates may include regularly reviewing the information provided on the Online Safeguarding section of the LSCB website which includes a dedicated section for Schools & Colleges as well as a *News & Events* area and *Focus On…* sections.

Resources

Highly Recommended

LSCB > Dedicated Lancashire Online Safety Website

Dedicated online safety section for Schools and Colleges

www.lancashiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce

Staff training

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.

85. In addition all staff should receive regular safeguarding and child protection updates (for example, via email, e-bulletins, staff meetings), as required, and at least annually, to provide them with relevant skills and knowledge to safeguard children effectively.

86. 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.

Advice

Research regularly informs us that staff training for schools is typically the weakest area of provision when assessing Online Safety. Safeguarding and child protection training provided to all staff on induction (and at least annually), should include Online Safety and is further explained on pages 26 & 34 of this guidance. Regular updates may include using the Safeguarding Board's 7-Minute Briefing resources (which include online safety-related topics) or by attending sessions such as those offered by the LSCB.

Resources

LSCB > Learning & Development

Useful and wide variety of safeguarding courses and learning resources including online safety and the very popular 7-Minute Briefing series

www.lancashiresafeguarding.org.uk/learning-development

Advice

Examples of good practice therefore 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 staff training calendar.

Advice

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. This aspect is referred to in more detail on pages 26 & 27 of this guidance.

Lancashire Safeguarding Children Board in partnership with UKSIC colleagues provide a free-of-charge yearly 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 (2-hour), sharp update on current aspects and trends around Online Safety for the Children's workforce - DSLs are strongly advised to attend wherever possible.

Resources

LSCB & UKSIC > Online Safety Live (in Lancashire) Briefing Session
Extremely popular, highly-recommended 2-hour annual event in January hosted by Lancashire Safeguarding Boards and delivered by the UK Safer Internet Centre
www.lancashiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce#DatesEvents

---

Online safety

87. 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 [to] keep their children safe online is provided in Annex C.

Advice

Emphasis on the responsibilities of Governing bodies/Proprietors is again apparent and this re-iterates that Online Safety is viewed as part of school and college 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 essential to recognise that whilst these are important supporting tools, they are 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 online access. Further information and recommendations on this aspect are available on pages 16 & 30-33 of this guidance
As in both the 2016 & 2018 revisions, Online Safety continues to have a dedicated Annex (Annex C) for Online Safety which is referred to on page 28 of this guidance. This is indicative of:

- the importance placed on ensuring Online Safety is appropriately addressed;
- that Online Safety is firmly identified as a Safeguarding issue;

Opportunities to teach safeguarding

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.

Advice

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, for example, limited to the Computing aspects. Online Safety education should start within early years and be progressive 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.

Relatedly, one of the main barriers to effective online safety education is in ensuring learning is progressive and age-appropriate across phases. In addition, the repetition of (albeit useful) resources will typically lead to disengagement by pupils resulting in messages being viewed as irrelevant, outdated or not-in-touch with current challenges. In line with this, UKCIS has developed an extremely useful resource (Education for a Connected World) which can provide much-needed structure and importantly, progression across a number of related online themes.

Resources

Education for a Connected World

A framework to equip children and young people for digital life

UKCIS

Lancashire Safeguarding Boards ✓✓✓✓✓ Very Highly Recommended

UKCIS > Education for a Connected World

Excellent and very highly-recommended framework set across 8 online safety themes highlighting progressive levels for Early Years – 7; 7 – 11 y/o; 11 – 14 y/o and 14 – 18 y/o.

www.gov.uk/government/publications/education-for-a-connected-world

Advice

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 visitors 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 Relationships & Sex Education (RSE) should be a key aspiration and will support a longer-term approach, including building resilience and the capacity to respond to concerns as they arise.

Advice

Where external visitors are utilised, careful consideration should be paid to selecting those with current knowledge, specific expertise and relevant experience. Research demonstrates a 'scaremongering' approach is typically counter-productive and can adversely lead to further traumatizing those who may have experienced related issues. Good practice shows that where external visitors are intended for a classroom setting, it is useful to remember that they should be viewed as an 'education resource' to support curriculum delivery rather than as a 'substitute teacher'. UKCIS colleagues have produced useful guidance for schools considering using external visitors with practical advice and recommendations.

Relatedly, viral scare stories, online challenges and fake news stories being circulated through Social Media become ever-more common. Viral scare stories in particular (sometimes referred to as *Digital Ghost Stories*) rely on concerned users drawing attention to the issue without checking their veracity beforehand and albeit well-intentioned, this further exacerbates the issue causing additional distress and anxiety, particularly for younger children. Unscrupulous marketing opportunities have also been seen to take advantage of further publicising such scare stories and therefore developing digital resilience for children and young people (and adults across the children's workforce) is an ever more important aspect of effective online safety provision.

Resources

UK Council for Internet Safety

Using External Visitors to Support Online Safety Education

July 2018

UKCIS > Using External Visitors to Support Online Safety Education
Useful guidance when considering using external visitors in school (July 2018)
www.gov.uk/government/publications/using-external-visitors-to-support-online-safety-education-guidance-for-educational-settings

Useful Note: if encountering problems with Adobe Acrobat, try opening with Google Chrome instead

Resources

ONLINE CHALLENGES

Appropriately supporting discussions about online scare stories

LSCB > Online Challenges – '*Think Before You ~~Share~~ Scare*' Template Letter
A useful template letter which can be adapted and used to address viral online scare stories with parents and carers (February 2019)
www.lancashiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce#challenges

Advice

Effective Online Safety education should be embedded across the curriculum, including through PSHE and Computing subject areas 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.

Resources

Key principles of effective prevention education

PSHE Association

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

Resources

Childnet > Crossing the Line Toolkit (11-14 y/o): PSHE Resource
Very useful PSHE toolkit resource with themes including: Cyberbullying; Sexting; Peer Pressure; Self-Esteem;
www.childnet.com/resources/pshe-toolkit/crossing-the-line

Advice

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, which can be an invaluable tool to aid in planning curriculum activity and selecting supporting resources.

Resources

Highly Recommended

SWGfL > Digital Literacy & Citizenship Resources
Highly Recommended (freely-available) classroom resources
www.digital-literacy.org.uk

Advice

As previously highlighted, the school/college Online Safety curriculum should be flexible, relevant, engage pupils' interests, be appropriate to their own needs and abilities and encourage pupils to develop resilience to online risks. Schools and colleges should use a range of relevant resources and be mindful that Online Safety education content can become dated very quickly due to the rapid pace of change within technology. Good practice demonstrates that where schools and colleges ensure learners are involved in developing the Online Safety curriculum, its content is current, relevant and is better able to ensure their concerns are being covered. This may involve engaging with pupil/student councils or include elements of peer education where appropriate. The LSCB MyAdvice Project referred to on pages 26-27 of this guidance provides an excellent child-centric insight that can support this aspect.

Resources

Childnet International

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

Resources

THINK U KNOW .co.uk

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

Resources

Department for Education

Teaching online safety in school

Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects

June 2019

DfE > Teaching online safety in school (June 2019)
Guidance to support schools to teach pupils how to stay safe online within new and existing school subjects
www.gov.uk/government/publications/teaching-online-safety-in-schools

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.

Advice

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 safeguarding 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 as such, 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 provide the facility to allow schools to individually customise filtering policies according to local requirements such as by a user group or key stage and will help to address '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 important information, suggested resources and recommended good practice around filtering and monitoring aspects are included on pages 30-33 of this guidance.

Inspection

91. From September 2019, Ofsted's inspections of early years, schools and post-16 provision will be carried out under: Ofsted's Education Framework. Inspectors will always report on whether or not arrangements for safeguarding children and learners are effective. In addition to the Framework and Inspection handbooks, Ofsted publishes specific guidance to inspectors on inspecting safeguarding: Inspecting safeguarding in early years, education and skills. The Independent Schools Inspectorate (ISI) is approved to inspect certain independent schools, and will also report on safeguarding arrangements. ISI has a published framework which informs how they inspect at Independent Schools Inspectorate.

Advice

Ofsted's Education Inspection Framework (EIF) includes handbooks for a variety of settings. Each handbook includes different references to online safety but it is clear that there should be effective arrangements to help pupils and students protect themselves online within the setting's Safeguarding arrangements. Schools and Colleges may wish to audit current practice to identify strengths and areas for improvement using the very-highly recommended SWGfL 360° Safe self-review tool highlighted on page 9 of this guidance.

Resources

Ofsted
raising standards
improving lives

School inspection handbook

Handbook for inspecting schools in England under section 5 of the Education Act 2005

Ofsted > Education Inspection Framework (Inspection Handbooks) (from September 2019)
Setting-specific inspection guidance for Ofsted inspectors from September 2019
www.gov.uk/government/collections/education-inspection-framework

Peer on peer abuse

97. **All** staff should recognise that children are capable of abusing their peers. All staff should be clear about their school's 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:

[…]

- the different forms peer on peer abuse can take, such as:
  - sexual violence and sexual harassment. Part five of this guidance sets out how schools and colleges should respond to reports of sexual violence and sexual harassment;

  […]

- sexting (also known as youth produced sexual imagery): the policy should include the school's 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; and

Advice

This section 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 UKCIS resources highlighted under 'Specific Safeguarding Issues' on pages 5-6 above are excellent supporting resources to support Schools and Colleges with this aspect. Where escalation of Sexting incidents to the Police are required (Note: see LSCB flowchart advice resource on page 6), this should follow defined safeguarding procedures (i.e. escalation through the Designated Safeguarding Lead).

Resources

Department for Education

Searching, screening and confiscation

Advice for headteachers, school staff and governing bodies

January 2018

DfE > Searching, screening and confiscation advice (January 2018)
Guidance for staff and school leaders
https://www.gov.uk/government/publications/searching-screening-and-confiscation

Children with special educational needs and disabilities

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.

Advice

Research informs us that children with special educational needs or disabilities can be particularly vulnerable to the risks posed by the online world. Ensuring policies and procedures reflect this particular aspect may include specific statements in this regard and as part of a whole-school approach, the inclusion of the SENCO in their development is recommended. Understanding that phrases and terminology can be interpreted in different ways is a useful consideration and colleagues at Kent County Council have produced a useful guide that can support this aspect.

Resources

kelsi Kent County Council

Online Safety for Learners with Special Educational Needs and Disabilities (SEND)

Kent County Council > Online Safety for Learners with SEND (November 2018)
Useful guidance when considering online safety for those with Special Educational Needs and Disabilities
www.kelsi.org.uk/__data/assets/pdf_file/0011/74576/Online-Safety-for-SEND.pdf

Part four: Allegations of abuse made against teachers and other staff

Confidentiality

214. The legislation imposing restrictions makes clear that "publication" of material that may lead to the identification of the teacher who is the subject of the allegation is prohibited. "Publication" includes "any speech, writing, relevant programme or other communication in whatever form, which is addressed to the public at large or any section of the public." This means that a parent who, for example, published details of the allegation on a social networking site would be in breach of the reporting restrictions (if what was published could lead to the identification of the teacher by members of the public).

Advice

School colleagues regularly cite parental engagement as the most common challenge schools face when addressing online safety. Where managed appropriately, engagement through Social Media can be a very useful tool in this regard. However, expectations for the wider school community should be made explicitly clear.

It is often useful to remember that where employed, Social Media should be used to enhance and support other forms of engagement rather than replace them (e.g. Parental sessions, complaints processes).

Part five: Child on Child Sexual Violence and Sexual Harassment

254. As per Part one of this guidance, all staff should be trained to manage a report […]

[…]

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

Advice

Experience shows that even with the best of intentions, managing instances of sexting can be problematic. The UKCIS Sexting advice for schools and colleges contains some extremely useful advice and practical step-by-step guidance on managing instances of sexting (see link on page 6 of this guidance).

As also highlighted on page 6 of this guidance, Lancashire Safeguarding Boards have published supporting local guidance on managing sexting instances including criteria for local handling and where (if appropriate) escalation to external partners such as the Police may be required.
Para 261 identifies the different options available to schools and colleges in managing reports including: Manage internally; Early Help; Referrals to children's social care; Reporting to the Police; - each of these options is further clarified on pages 69-71 of the KCSIE guidance.

Note: It is very strongly recommended that all DSLs should be expressly familiar with the UKCIS Sexting advice highlighted on page 6 of this guidance.

Resources

Department for Education

Sexual violence and sexual harassment between children in schools and colleges

May 2018

DfE > Sexual violence and sexual harassment guidance (May 2018)
Useful guidance for Governors, Headteachers, SLTs & DSLs including minimising the risk of occurrence and what to do in the event of an instance or allegation
www.gov.uk/government/publications/sexual-violence-and-sexual-harassment-between-children-in-schools-and-colleges

The end of the criminal process

[. . .]

- Any conviction (even with legal anonymity reporting restrictions) is potentially going to generate interest among other pupils or students in the school or college. It will be important that the school or college ensure both the victim and alleged perpetrator remain protected, especially from any bullying or harassment (including online).

Advice

Additionally, page 73 of KCSIE above highlights the need for protection in relation to publicity for both the alleged perpetrator and victim. This is particularly relevant where students may potentially circulate information via Social Media and expectations in this regard should be explicitly clear. This may be referred to in the school/college's Acceptable Behaviour Agreement which should outline expected standards of behaviour both within and outside of the school environment.

Para 262 includes a variety of principles to consider when safeguarding and supporting the victim as well as potential areas of support. These include reference to the Internet Watch Foundation (IWF) who may be able to support removing illegal images.

Resources

IWF > Removing illegal content

Anonymous reporting portal provided by the Internet Watch Foundation to report child abuse images and content.

https://report.iwf.org.uk/en

Annex A: Further information

Child sexual exploitation

Child sexual exploitation is a form of child sexual abuse. It occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into sexual activity (a) in exchange for something the victim needs or wants, and/or (b) for the financial advantage or increased status of the perpetrator or facilitator. The victim may have been sexually exploited even if the sexual activity appears consensual. Child sexual exploitation does not always involve physical contact: it can also occur through the use of technology. Like all forms of child sex abuse, child sexual exploitation:

- can affect any child or young person (male or female) under the age of 18 years, including 16 and 17 year olds who can legally consent to have sex;
- can still be abuse even if the sexual activity appears consensual;
- can include both contact (penetrative and non-penetrative acts) and non-contact sexual activity;
- can take place in person or via technology, or a combination of both;
- can involve force and/or enticement-based methods of compliance and may, or may not, be accompanied by violence or threats of violence;
- may occur without the child or young person's immediate knowledge (e.g. through others copying videos or images they have created and posted on social media);
- can be perpetrated by individuals or groups, males or females, and children or adults […]

Advice

Annex A contains additional information about specific forms of abuse and includes the addition of a useful index section. Child Sexual Exploitation (CSE) may involve utilising the Internet and Social Media to identify potential victims or as a tool to coerce or blackmail children into performing sexual acts, both online and offline. Means of accessing the Internet may also be provided to the child or young person 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 remains a useful resource 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.

Resources

CEOP > ThinkUKnow (TUK) ‘Exploited’ Resource
TUK CSE Prevention Resource
www.thinkuknow.co.uk/professionals/resources/exploited

Resources

Lancashire Safeguarding Boards
Highly Recommended

CEOP > Click CEOP Button
CEOP Safety Centre – Click CEOP reporting button. Useful to include on websites and reference when addressing CSE-related topics
www.ceop.police.uk/safety-centre

Preventing radicalisation

Children are vulnerable to extremist ideology and radicalisation. Similar to protecting children from other forms of harms and abuse, protecting children from this risk should be a part of a schools' or colleges' safeguarding approach.

[…] Radicalisation[106] refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

There is no single way of identifying whether a child is likely to be susceptible to an extremist ideology. Background factors combined with specific influences such as family and friends may contribute to a child's vulnerability. Similarly, radicalisation can occur through many different methods (such as social media) and settings (such as the internet).

[…]

The Prevent duty

All schools and colleges are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015 (the CTSA 2015), in the exercise of their functions, to have "due regard[107] to the need to prevent people from being drawn into terrorism".[108] This duty is known as the Prevent duty.

The Prevent duty should be seen as part of schools' and colleges' wider safeguarding obligations. Designated safeguarding leads and other senior leaders should familiarise themselves with the revised Prevent duty guidance: for England and Wales […] The guidance is set out in terms of four general themes: Risk assessment, working in partnership, staff training, and IT policies.

Advice

This section acknowledges the increasing 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. Whilst it is not necessary to have a separate 'Prevent' policy, responding to radicalisation should be set out in existing Safeguarding policies. DSLs should be familiar with the statutory requirements of the Government's Prevent Duty 2015. 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).

Freely available supporting resources around the broader radicalisation/extremism agenda continue to be available on the highly-popular Lancashire preventforschools.org website. This includes specific guidance produced for schools around Online Radicalisation.

Resources

P4S > Lancashire preventforschools.org website
Very popular Lancashire site providing access to a range of (freely available) primary and secondary classroom resources to address radicalisation/extremism.
www.preventforschools.org

Resources

LSCB > 7-Minute Briefing (Online Radicalisation) - July 2018
Useful short summary information from Lancashire Safeguarding Boards designed to be used in Staff Briefing sessions
www.lancashiresafeguarding.org.uk/learning-development/7-minute-briefings

Resources

P4S > Online Radicalisation
Useful information from the Lancashire P4S site around Online Radicalisation and its relation to the broader online safety agenda
www.preventforschools.org/?category_id=55

Resources

SWGfL > SELMA Toolkit (Online Hate Speech)
A very useful collection of activities, resources and lesson plans to support those working with young people aged 11-16 to understand online hate speech
https://hackinghate.eu/

Resources

Childnet > Trust Me (Thinking critically about what you see online)
Very Highly Recommended Primary & Secondary resources to support building online resilience through Digital Literacy
www.childnet.com/resources/trust-me

Lancashire Safeguarding Boards
Very Highly Recommended

Advice

The Prevent Duty guidance highlights four main themes including IT policies. 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 30-33 of this guidance 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.
Should the filtering system used in school be changed, this should be reviewed and incorporated into the school's associated Prevent Duty Risk Assessment. It is recommended that filtering systems chosen should meet the above national standards and as a minimum, must implement "*the police assessed list of unlawful terrorist content, produced on behalf of the Home Office*".

Further information and useful advice on how to check and evidence filtering provision is provided on page 32 of this guidance.

Peer on peer abuse

Children can abuse other children. This is generally referred to as peer on peer abuse and can take many forms. This can include (but is not limited to) bullying (including cyberbullying); sexual violence and sexual harassment; physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm; sexting and initiating/hazing type violence and rituals.

Sexual violence and sexual harassment between children in schools and colleges

Context

Sexual violence and sexual harassment can occur between two children of **any** age and sex. It can also occur through a group of children sexually assaulting or sexually harassing a single child or group of children.

[…] Sexual violence and sexual harassment exist on a continuum and may overlap, they can occur online and offline (both physical and verbal) and are never acceptable. It is important that **all** victims are taken seriously and offered appropriate support. Staff should be aware that some groups are potentially more at risk. Evidence shows girls, children with SEND and LGBT children are at greater risk.

[…]

Advice

First introduced in the 2018 revisions to KCSIE, Peer on peer abuse and Sexual violence and sexual harassment between children in schools and colleges, both include a number of online elements. These sections highlight aspects of peer-on-peer abuse and sexual violence/sexual harassment, including that this can take place between children of any age and sex and may include groups of children harassing a single child or group.
Additionally, it includes reference to particular groups being potentially more at risk such as girls, children with SEND and LGBT children.

Within the definitions of sexual harassment, there is specific reference to online sexual harassment including non-consensual sharing of images/videos, sexualised online bullying, sexualised comments on social media and sexual exploitation through coercion and threats.

Experience demonstrates that it is essential that the initial response to a report from a child is very important and the section gives useful guidance in this respect along with a variety of additional sources of support.

Good practice includes ensuring both policies and procedures have a child-centric focus with robust systems that can be clearly understood and followed by all staff.

Upskirting[113]
'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.

Advice

The 2019 revisions to KCSIE sees the introduction of a new section on 'Upskirting'. *Upskirting* typically involves the use of a device with a camera (such as a smartphone) to take a photograph or video under the subject's clothing without their knowledge. All staff should be made aware of what *Upskirting* is, and that it became a criminal offence in April 2019 punishable by up to 2 years in prison.

Annex B: Role of the designated safeguarding lead

Governing bodies, proprietors and management committees should ensure an appropriate **senior member** of staff, from the school or college **leadership team**, is appointed to the role of designated safeguarding lead.[114] The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection (including online safety). […]

The designated safeguarding lead is expected to:

[…]

- liaise with staff (especially pastoral support staff, school nurses, IT Technicians, and SENCOs or the named person with oversight for SEN in a college) on matters of safety and safeguarding (including online and digital safety) […]

Advice

As previously highlighted, Online Safety is primarily a safeguarding issue and this is re-enforced through the inclusion of online safety as a lead responsibility for the Designated Safeguarding Lead.

This section highlights a number of aspects including managing referrals and working with others. This latter point is particularly relevant in the online context and highlights the expectation of liaising with related staff such as the IT Technician or SENCO.

Training

The designated safeguarding lead (and any deputies) should undergo training to provide them with the knowledge and skills required to carry out the role. This training should be updated at least every two years. The designated safeguarding lead should undertake Prevent awareness training.

In addition to the formal training set out above, their knowledge and skills should be refreshed […] as required, and at least annually, to allow them to understand and keep up with any developments relevant to their role so they:
[…]

- understand and support the school or college with regards to the requirements of the Prevent duty and are able to provide advice and support to staff on protecting children from the risk of radicalisation;

- 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;

- encourage a culture of listening to children and taking account of their wishes and feelings, among all staff, in any measures the school or college may put in place to protect them.

Advice

Whilst formal DSL training should be updated at least every two years (and include online safety), knowledge and skills should be refreshed at least annually and this is particularly relevant to the online environment given the pace of its continual progression and development. The (free-to-attend) Online Safety Live (OSL) events hosted annually by the Safeguarding Boards in January are an excellent way to support this requirement and remain updated on current risks and best practice and it is strongly recommended DSLs attend wherever possible.

Resources

LSCB & UKSIC > Online Safety Live (in Lancashire) Briefing Sessions
Extremely popular, very highly-recommended 2-hour events held in January each year, hosted by Lancashire Safeguarding Boards and delivered by our colleagues from the UK Safer Internet Centre

www.lancashiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce.aspx#DatesEvents

Advice

Developing a culture of listening to C&YP's views will help to ensure online safety education is current and relevant and will include those areas they would like more information about. The LSCB MyAdvice schools-based project took a broad-scale approach to secure the views of C&YP across the Lancashire region and the resulting summary animation provides invaluable information and can be used as a stimulus to developing similar local activities in school.

Resources

Lancashire Safeguarding Boards
MyAdvice
summary findings (visual) report
listening to young people's views about the online world

LSCB > LSCB MyAdvice Project 2018/19
LSCB 'Voice-of-the-Child' project to elicit the views of Lancashire's C&YP about Online Safety, including recommendations and peer advice
www.lancashiresafeguarding.org.uk/online-safeguarding/myadvice

Raise Awareness

The designated safeguarding lead should:

[…]

- link with the safeguarding partner arrangements to make sure staff are aware of any training opportunities and the latest local policies on local safeguarding arrangements.

Advice

Maintaining links with the revised safeguarding partner arrangements is highlighted as a role for the DSL. The Safeguarding Board also has the previously mentioned dedicated Online Safeguarding section on its website (with a specific section for the children's workforce) to promote both consistent and current advice, providing a wide variety of quality-assured resources, courses and events such as the previously mentioned OSL sessions.

In addition, the Safeguarding Board has a dedicated Learning & Development Team which incorporates an array of wider safeguarding-related resources and courses relevant to DSLs.

Resources

Lancashire Safeguarding Boards Website
Teachers & Professionals

Highly Recommended

LSCB > Dedicated Lancashire Online Safety Website
Dedicated online safety section for Schools and Colleges
www.lancashiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce

Resources

Lancashire Safeguarding Boards
Learning & Development
7-Minute Briefings
Brief safeguarding sp variety of topics.
Training Ev
A full list of courses can be viewed by follo
7 Minute Briefings

LSCB > Learning & Development Website
Learning & Development website from Lancashire Safeguarding Boards including 7-Minute Briefings and Training opportunities
www.lancashiresafeguarding.org.uk/learning-development

Annex C: Online Safety

The dedicated Annex for Online Safety (Annex C) first introduced in the 2016 revision to KCSIE has again seen a number of revisions for 2019 and continues to include a specific Education section first introduced in 2018.

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 in and escalate any incident where appropriate.

Advice

This again 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; 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.

Advice

The '3C's Risk Matrix' was originally identified through the LSE 'EU Kids Online' project and is also referred to in the Pan-Lancashire LSCB Online Safeguarding Strategy as a useful means of categorising risk areas according to type. The information includes a number of examples of potential issues identified according to each risk area although it is important to recognise that these are not mutually exclusive (e.g. extremist content can also apply to 'Conduct' as well as 'Content').

Resources

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/overview

Education

Opportunities to teach safeguarding, including online safety, are discussed at paragraph 88-90. Resources that could support schools and colleges include:

- Teaching online safety in school – DfE guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.

- UKCCIS has recently published its *Education for a connected world framework*. Online safety is a whole school and college issue. The framework aims to support the development of the curriculum and is of particular relevance to PSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond and to be central to a whole school or college approach to safeguarding and online safety. It covers early years through to age 18.

- The PSHE Association provides guidance to schools on developing their PSHE curriculum – www.pshe-association.org.uk

- Parent Zone and Google have developed Be Internet Legends a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils.

Advice

As previously highlighted through the MyAdvice project, good practice 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 15 is an excellent resource to support this aspect.

This section, first introduced in 2018, builds upon the information in paras 88-90 and highlights a number of very useful resources. The 2019 update sees the introduction of '*Teaching Online Safety in School*' – a useful reference released in June 2019 outlining how schools can implement Online Safety within new and existing curriculum requirements.

As in 2018, of particular note is the reference to the UKCIS framework '*Education for a Connected World*' originally highlighted on Page 13 of this resource. This resource continues to be very highly-recommended and extremely useful when planning curriculum delivery that is both age-appropriate and progressive.

Resources

Department for Education

June 2019

Teaching online safety in school

Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects

DfE > Teaching online safety in school (June 2019)
Guidance to support schools to teach pupils how to stay safe online within new and existing school subjects
www.gov.uk/government/publications/teaching-online-safety-in-schools

Resources

Education for a Connected World

A framework to equip children and young people for digital life

UKCIS

UKCIS > Education for a Connected World (February 2018)

Excellent and very highly-recommended framework set across 8 online safety themes highlighting progressive levels for Early Years – 7; 7 – 11 y/o; 11 – 14 y/o and 14 – 18 y/o.

www.gov.uk/government/publications/education-for-a-connected-world

Resources

SWGfL > Swiggle Child Friendly Search Engine

An excellent search engine facility with additional features (e.g. screen cover) developed by SWGfL. It is particularly recommended for those working with younger children as the default homepage setting for school devices

https://swgfl.org.uk/services/swiggle/

Advice

Integrating Online Safety as a whole-school approach remains essential and increasingly applies to broader curriculum aspects. The recently revised Relationships, Sex & Health curriculum helps to underline that Online Safety should extend beyond the historical Computing curriculum approach if it is to be effective. The revised Relationships curriculum for 2020 has very significant and much-welcomed links to numerous aspects of Online Safety including social media, information sharing, online relationships, online games and importantly, health and wellbeing.

Resources

Department for Education

February 2019

Relationships Education, Relationships and Sex Education (RSE) and Health Education

Draft statutory guidance for governing bodies, proprietors, head teachers, principals, senior leadership teams, teachers

DfE > RSE Curriculum

Statutory guidance from September 2020 with multiple references across both the Primary and Secondary phases to various aspects of Online Safety

www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education

Filters and monitoring

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

Whilst considering their responsibility to safeguard and promote the welfare of children, and provide them with 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 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.[117] The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like: UK Safer Internet Centre: appropriate filtering and monitoring

[…]

Advice

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 (UKSIC) has 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, including whether the preferred provider has engaged with the UKSIC self-certification scheme (see links below).

Resources

UK Safer Internet Centre
Appropriate Filtering & Monitoring
updated

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

UK Safer Internet Centre
Appropriate Filtering & Monitoring
updated

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

Advice

It is important to recognise that a content filtering system will mitigate access to inappropriate content rather than remove it. However, there are core requirements that should prevent access to illegal content such as child abuse images and unlawful terrorist content. Checking and evidencing that the school or college's filtering system fulfils this requirement can be achieved by utilising the excellent Content Filter Checking Utility tool developed by our colleagues at the South West Grid for Learning. This newly-released tool allows education establishments to easily check compliance by running a check on the school or college system against a variety of lists including the *Child Abuse Images and Content (CAIC)* list maintained by the Internet Watch Foundation and the previously mentioned *'police assessed list of unlawful terrorist content, produced on behalf of the Home Office'*, highlighted on page 23 of this guidance.

It is therefore strongly recommended that schools and colleges should make use of this freely-available utility to check and evidence the compliance of the chosen filtering system on a regular basis alongside using the UKSIC guidance on appropriate filtering and monitoring.

Resources

Highly Recommended

SWGfL > Filter-checking Utility
Freely-available content filtering utility used to evidence compliance with recommended filtering requirements
http://testfiltering.com

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

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

Advice

As highlighted previously, filtering and monitoring systems should NOT be considered as 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.

Advice

Whilst not necessary in all settings, where monitoring *software* is employed, effective practice includes ensuring reports are sent to the Safeguarding lead (as opposed to just the ICT lead) as this helps to ensure potentially wider safeguarding concerns (i.e. non-ICT related) are considered.

It is essential that all Governing bodies, proprietors and members of staff recognise that even with the most costly and up-to-date security and filtering systems, children or staff can potentially bypass them by various means including 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, 4G & 5G connectivity by focusing on what is acceptable behaviour rather than what device is used and whether or not it is owned by the school/college.

Reviewing online safety

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

Advice

Experience shows that whilst there is typically focus on Policies/Procedures, Technology and Education, the associated emphasis on reviewing the effectiveness of provision can sometimes be overlooked.
As referred to on page 9 of this guidance, the 360° Safe Self-Review Tool produced by colleagues at SWGfL is highly recommended and provides schools and colleges with a freely-available means to self-evaluate provision. The award-winning tool includes a number of 'benchmarks' and suggested options for further progression.

In addition, Governors & Proprietors have a key role in ensuring that Online Safety provision is appropriate and effective. To support with this, the Board has developed a Self-Review Tool for Governors & Proprietors which complements the UKCIS 'Questions for the Governing Board' guidance. Again, very popular both within and outside of the Lancashire region, the Self-Review Tool identifies a number of 'inward' and 'outward' facing questions to support ensuring effective provision.

Resources

LSCB
Online Safety
Governance
Checklist
☑ Review
☐ Guidance
☑ for Governors
& Proprietors

LSCB > Governor Online Safety Self-Review Tool (August 2019)
LSCB prompts to support Governors & Proprietors when review Online Safety provision in their settings
www.lancashiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce#GovernorSRT

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 safety (paragraph 87), that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Advice

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 and Schools and Colleges are best placed to decide how this is implemented within their own setting. Additionally, given the continually evolving nature of Online Safety, all staff should receive updates on a regular basis, for example as a standing safeguarding agenda or team briefing item. As in previous years, research continues to inform us that staff training is typically the weakest area of Online Safety in schools. Good practice suggests whole-school awareness training should be completed (at least) every two years and those with a specific responsibility (e.g. DSL, Online Safety lead) should receive specific updates at least annually. Whilst they will each have a distinct focus, it is suggested that staff training is considered when planning for Parental Awareness Sessions (e.g. Staff Session followed by Parental Session) to both ensure consistency and potentially save costs if procuring external expertise.

Whilst the preference for training would be to deliver from within exisiting resource in the School/College (e.g. Online Safety Group member), it is recognised that this is not always feasible (e.g. where a more in-depth understanding of the issues is needed or where an external authority may be preferable). The use of external agencies to provide training should be carefully considered, bringing both positive and negative considerations and therefore, the UKCIS advice referred to on page 14 of this guidance can be very helpful in this regard.

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 presence can be a challenge, 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 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 about available training courses, opportunities and enquiries can be found via the LSCB website in both the Learning & Development and dedicated Online Safeguarding sections.

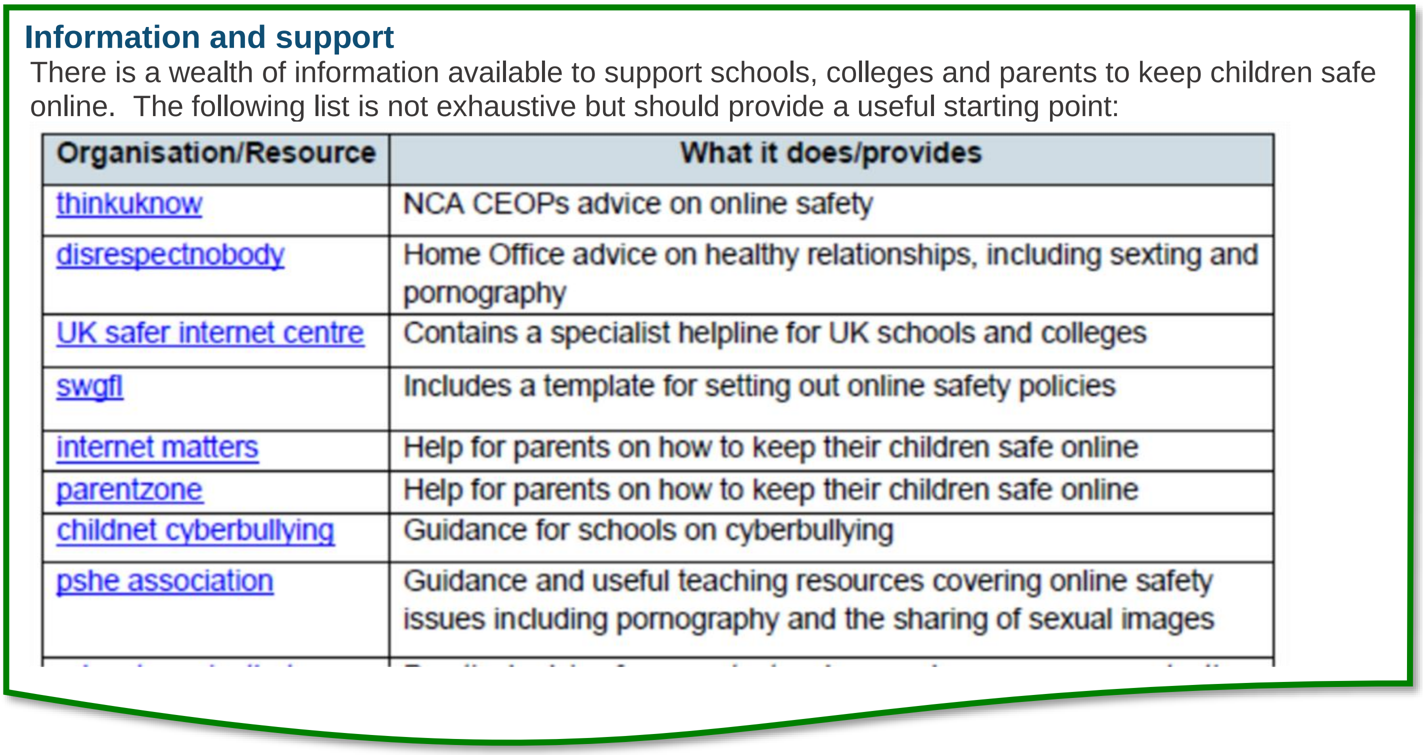
Resources

LSCB > 7-Minute Briefing (Social Media & Mental Health) – February 2019
Useful short, summary snapshot about Social Media and Mental Health & Wellbeing
www.lancashiresafeguarding.org.uk/learning-development/7-minute-briefings

Resources

Learning & Development
Safer Online Behaviours Course (Children)
Lancashire Safeguarding Boards

LSCB > Learning & Development Courses and Events
Information about the variety of training events provided through the LSCB L&D service
www.lancashiresafeguarding.org.uk/learning-development



Information and support

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

Organisation/Resource	What it does/provides
thinkuknow	NCA CEOPs advice on online safety
disrespectnobody	Home Office advice on healthy relationships, including sexting and pornography
UK safer internet centre	Contains a specialist helpline for UK schools and colleges
swgfl	Includes a template for setting out online safety policies
internet matters	Help for parents on how to keep their children safe online
parentzone	Help for parents on how to keep their children safe online
childnet cyberbullying	Guidance for schools on cyberbullying
pshe association	Guidance and useful teaching resources covering online safety issues including pornography and the sharing of sexual images

Advice

On page 98, KCSIE introduces a sample of useful sources of support. One of the challenges most commonly highlighted by school colleagues is what resources to use when addressing online safety. The online environment continually develops and resources can become outdated quickly. This was particularly reflected during the LSCB MyAdvice project where C&YP highlighted that the repeated use of the same resources or resources that are viewed to be out-of-date is a significant barrier to effective engagement and learning. As well as currency, choosing good-quality resources from the wide array available is also a significant challenge. Along with those resources highlighted within this *Making Sense of…* guidance, the Safeguarding Board's dedicated Online Safeguarding section aims to signpost a variety of quality-assured resources from reputable providers. The site is regularly updated to reflect a current and consistent approach with recommended tools to support delivery. It also includes a variety of other useful information such as News, Events, FAQs and resources to support Parents, Carers and the wider school community.

Resources

LSCB > Dedicated Lancashire Online Safety Website
Dedicated online safety section for Schools and Colleges
www.lancashiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce

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. Providing a balanced and whole-school curriculum approach remains a key element and in particular, both RSE and PSHE practitioners have increasingly important opportunities to contribute to progressing this area of safeguarding provision. Equally, supporting our Children and Young People to stay safe online equips them with lifelong skills that will extend far beyond the academic environment. It is therefore immensely important that we provide them with the knowledge and skills to become digitally resilient learners, protecting them both against today's risks and those online challenges to come that may not yet be apparent.

It is clear that this aspect of Safeguarding continues to evolve and develop at a pace but it is essential to recognise that issues around online safety are fundamentally Safeguarding rather than ICT concerns and therefore, our approach should reflect this and not be distracted by the involvement of technology. All of the above highlighted resources are available via the *Supporting Resources* section of the LSCB website below and whilst this guidance does not seek to be exhaustive, it is intended to provide colleagues with support and guidance when developing School and College Online Safety provision.

We hope you continue to find this a useful, informative and productive resource.

Graham Lowe
Online Safeguarding Advisor
Chair, Pan-Lancashire LSCB Online Safeguarding Group
August 2019

✉ graham.lowe2@lancashire.gov.uk
⌂ www.lancashiresafeguarding.org.uk

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

Acknowledgements: This guidance has been developed to support schools and colleges in progressing the Online Safeguarding aspects of the revised DfE Keeping Children Safe in Education statutory guidance 2019. Advice has been referenced from a variety of school colleagues and organisations and collates useful recommendations and experience of good practice.