Making Sense of...

Keeping children safe in education 2020

A practical guide for Schools and Colleges on those aspects of the statutory guidance relating to Online Safety, what they mean and how to address

: edition four : rev3620 :
September 2020

Children's
Safeguarding Assurance
Partnership
working together to stay safe online

Content Quick Links

*Making Sense of…*Keeping Children Safe in Education 2020

Introduction

In 2016, further to requests from Headteacher and Designated Safeguarding Lead colleagues across the region, Lancashire Safeguarding Children Board (now Children's Safeguarding Assurance Partnership (CSAP)) 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 2019, proving highly-popular amongst our colleagues in Schools and Colleges, both in the Lancashire region and beyond. With the release of the Keeping Children Safe in Education 2020, the Safeguarding Partnership has once again reviewed the statutory guidance in order to extract, clarify and provide updated guidance on those online safety-related areas as well as signposting recommended good-quality sources of support.

As in previous years, 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. Whilst not intended to be exhaustive, the following resource endeavours to highlight content that will be of particular interest to Governors, School Leaders and Designated Safeguarding Leads (DSLs).

Graham Lowe
CSAP/LSAB Online Safeguarding Advisor
Chair, Pan-Lancashire Online Safeguarding Group
Children's Safeguarding Assurance Partnership
September 2020

e-mail: graham.lowe2@lancashire.gov.uk
web: www.lancashiresafeguarding.org.uk
twitter: @LancsSguarding

Children's
Safeguarding Assurance
Partnership
working together to stay safe online

*Making Sense of…*KCSIE: Legend

123. **Example KCSIE extract**: a direct reference from the text within Keeping children safe in education (KCSIE) 2020. Specific references to Online Safety are highlighted for clarity. Text omitted for brevity from the original statement is denoted by the inclusion of square-bracket placeholders […]

Advice

Children's Safeguarding Assurance Partnership recommended advice and considerations relating to the preceding KCSIE extract. Advice may include references to other sections within the *Making Sense of…* guidance to avoid repetition.

Resources:

Example
Suggested
Resource
Lorem ipsum dolor sit amet, consectetuer adipiscing elit.
Children's Safeguarding Assurance Partnership

Organisation > Example Resource Title
A description of recommended, quality-assured resources identified to support progression. Resources identified are free of charge unless otherwise stated and include a direct weblink for ease of access
http://www.lancashiresafeguarding.org.uk

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.

[…]

22. **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. Children may be abused by an adult or adults or by another child or children.

24. **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) causing children frequently to feel frightened or in danger […]

Advice:

This clearly identifies that online or 'cyber' bullying is a form of emotional abuse. Schools and Colleges must 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 KS3 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.

25. **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 29).

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. Peer-on-peer abuse is further referenced on pages 7, 18 & 25 of this guidance.

Safeguarding issues

27. **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.

Child Sexual Exploitation (CSE) and Child Criminal Exploitation (CCE)

28. Both CSE and CCE are forms of abuse and both occur where an individual or group takes advantage of an imbalance in power to coerce, manipulate or deceive a child into sexual or criminal activity.

[…]

The abuse can be a one-off occurrence or a series of incidents over time, and range from opportunistic to complex organised abuse. It can involve force and/or enticement-based methods of compliance and may, or may not, be accompanied by violence or threats of violence. Victims can be exploited even when activity appears consensual and it should be noted exploitation as well as being physical can be facilitated and/or take place online. More information include definitions and indicators are included in Annex A.

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 and Child Sexual Exploitation. 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 platforms.

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 sexual exploitation, 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 and sending nudes
Advice to help you understand the risks and support your child if they've been sending, sharing or receiving nude images.

NSPCC > Sexting and sending nudes
Advice to help understand the risks of sending, sharing or receiving nude images
www.nspcc.org.uk/keeping-children-safe/online-safety/sexting-sending-nudes

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 follow established safeguarding procedures via the DSL. The UK Safer Internet Centre has 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 CSAP 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:

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

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

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

Very Highly Recommended
CSAP

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

CSAP > 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:

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 updated their very useful (freely available) resource *"So you got naked online…"* which provides practical advice and information for Young People experiencing issues.

Resources:

SWGfL > So you got naked online… (February 2020)
Useful supporting resource offering children, young people and parents advice to support the issues resulting from sexting incidents
https://swgfl.org.uk/resources/so-you-got-naked-online

Peer on peer abuse

29. **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.

30. 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), Upskirting and Sexting. Training should ensure that all members of staff are aware that not all online abuse is committed by adults or strangers, the education provided to children should reflect this and that staff clearly understand the school's policies and procedures in relation to peer-on-peer abuse.

Whilst this section highlights specific forms of abuse, Annex A of KCSIE provides further additional details on these and other forms of abuse and is referred to in greater detail on pages 22-26 of this guidance.

Mental Health

34. All staff should also be aware that mental health problems can, in some cases, be an indicator that a child has suffered or is at risk of suffering abuse, neglect or exploitation.

[…]

38. The department has published advice and guidance on Preventing and Tackling Bullying, and Mental Health and Behaviour in Schools (which may also be useful for colleges). In addition, Public Health England has produced a range of resources to support secondary school teachers to promote positive health, wellbeing and resilience among young people including its guidance Promoting children and young people's emotional health and wellbeing. Its resources include social media, forming positive relationships, smoking and alcohol. See Rise Above for links to all materials and lesson plans.

Advice:

The section on Mental Health is a new addition to KCSIE for 2020. As well as being a potential indicator of abuse, neglect, exploitation or other Adverse Childhood Experiences (ACEs), mental health issues can be linked to, and exacerbated by, the online environment. Promoting positive relationships and developing online resilience are key factors supporting emotional health and wellbeing - the Rise Above PSHE resources from Public Health England can be very useful in this regard and can support the curriculum from Upper Key Stage 2 through to Key Stage 4 with online-related topics including social media, cyberbullying, online stress, FOMO and body image in a digital world.

Resources:

Public Health England
RISE ABOVE FOR SCHOOLS
Tackling the challenges facing young people today
PSHE Association Quality Assured Resource
PSHE

Public Health England > Rise Above

Lesson plans and resources supporting a wide variety of aspects affecting physical and mental wellbeing

https://campaignresources.phe.gov.uk/schools/topics/rise-above/overview

Part two: The management of safeguarding

The responsibility of governing bodies, proprietors and management committees

Safeguarding policies and procedures

62. 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.

63. 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 Safeguarding Partnership has developed and updated a local summary self-review checklist resource to aid colleagues as part of their approach to addressing online safety provision.

Resources:

Online Safety Governance Checklist

☑ Review Guidance to support Governors & Proprietors

Children's Safeguarding Assurance Partnership working together to stay safe online

CSAP > Online Safety Governance Checklist: (updated Sept 2020)
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 (updated June 2020)
Useful updated 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 very 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.

Policy Tip: To aid in a robust, consistent and comprehensive approach, the Children's Safeguarding Assurance Partnership recommends Schools and Colleges make use of the SWGfL templates when developing or reviewing Online Safety policies. In addition, making use of the award-winning 360° Safe Self Review Tool to review and self-assess provision can help to support progression and identify potential areas for further development.

Resources:

SWGfL > Online Safety Policy Template
Excellent Online Safety Policy templates for Schools covering a wide range of policy issues
https://swgfl.org.uk/resources/online-safety-policy-templates

SWGfL > 360º Safe (Version 2.0) Online Safety SRT (updated April 2020)
Highly Recommended (freely available) Self Review Tool to support Schools with Online Safety review and progression
https://360safe.org.uk/

The designated safeguarding lead

67. 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 discrete aspects of Online Safety activities to other members of staff (e.g. where there is specific curriculum or technical knowledge/expertise required).

Addressing Online Safety effectively 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. This is 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.

70. The designated safeguarding lead and any deputies should liaise with the three safeguarding partners and work with other agencies in line with Working Together to Safeguard Children. […]

72. 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.

73. 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 Children's Safeguarding Assurance Partnership (formerly LSCB) maintains a strong commitment to Online Safeguarding, providing information, resources, training and briefings for partners across the children's workforce.

As identified in KCSIE para 73, it is important that DSLs access appropriate and regular updates to ensure their knowledge and skills remain current. The online environment continues to evolve and develop at a pace and therefore, DSLs must ensure their knowledge in this area is reflective 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 local and national policy and procedures. Informal updates may include regularly reviewing the information provided on the Online Safeguarding section of the CSAP website which includes a dedicated section for Schools & Colleges as well as a *News & Events* area and *Supporting Resources*.

More formally, this may include courses offered through the Safeguarding Partnership arrangements or from reputable external providers. Further information on these aspects including the annual Online Safety Live in Lancashire sessions can be found on pages 12 & 36 of this guidance.

Resources:

CSAP
Online
Safeguarding
Dedicated website section to support Teachers & Professionals
Children's
Safeguarding Assurance
Partnership
working together to stay safe online

CSAP > Lancashire Online Safeguarding Web pages

Dedicated online safety section to support colleagues in schools, colleges and the wider children's workforce

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

---

Staff training

89. 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.

90. 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.

91. 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 27 & 35 of this guidance. Regular updates may include using the CSAP 7-Minute Briefing resources (which include online safety-related topics) or by attending specific Online Safety sessions such as those offered by the CSAP.

Resources:

CSAP > Learning & Development
Useful wide range of safeguarding courses and learning resources for staff 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.

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 27 & 28 of this guidance.

The Children's Safeguarding Assurance Partnership (CSAP) in partnership with UKSIC colleagues have provided free-of-charge annual updates through the highly-popular annual Online Safety Live Briefings held at venues across the region each year in January. Whilst it does not replace the requirement for formal CPD training, the sessions provide an invaluable short (2-hour), sharp update on current aspects and trends around Online Safety for the Children's workforce.

Tip: Designated Safeguarding Leads in particular are strongly advised to attend one of the available sessions wherever possible.

Resources:

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

---

Online safety

92. 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 keep their children safe online (including when they are online at home) 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 & 32-34 of this guidance. This statement sees an addition for 2020 with a specific reference to the home environment: *"...governing bodies and proprietors keep their children safe online (including when they are online at home)..."* - this is addressed in more detail on page 35 of this guidance.

As in previous revisions, Online Safety continues to have a dedicated Annex (Annex C) for Online Safety which is referred to in detail on page 29 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

93. 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.

94. This may include covering relevant issues for schools through 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) which will be compulsory from September 2020. […] The following resources may help schools and colleges:

- DfE advice for schools: teaching online safety in schools
- UK Council for Internet Safety (UKCIS)[27] guidance: Education for a connected-world
- National Crime Agency's CEOP education programme: Thinkuknow
- Public Health England: Rise Above

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, current 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, the UKCIS has updated its extremely useful Education for a Connected World (EFACW) resource which can provide much-needed structure and importantly, progression across a number of related online themes.

Resources:

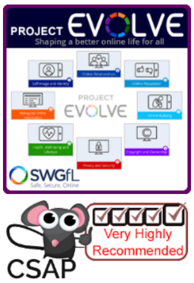
Education for a Connected World
A framework to equip children and young people for digital life
UK Council for Internet Safety
2020 edition
Very Highly Recommended
CSAP

UKCIS > Education for a Connected World **(2020 edition)**
Excellent & very highly-recommended progressive framework set across 8 online safety strands, highlighting levels for Early Years – 7; 7 – 11; 11 – 14 and 14 – 18 y/o.
www.gov.uk/government/publications/education-for-a-connected-world

Advice

Utilising the EFACW framework is strongly advised and provides a progressive and planned approach to online safety education. However, feedback suggests delivering those statements identified in the framework can be a challenge and as such, the recently developed Project Evolve Toolkit from the South West Grid for Learning (SWGfL) is very highly recommended. Project Evolve is mapped against the 300+ statements in the EFACW framework and holds a vast library of age appropriate content including ready-made activities, outcomes, supporting resources and professional development materials.

Resources:



SWGfL > Project Evolve Toolkit
A **very** highly-recommended (freely-available) toolkit mapped against the EFACW statements to support the delivery of age appropriate online safety education in schools and colleges from Early Years through to 18 y/o.
https://projectevolve.co.uk/

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

Where external visitors are utilised, careful consideration should be paid to selecting those with current knowledge, specific expertise and relevant education 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 or misleading news stories being circulated through Social Media become ever-more common and are unfortunately never far away from the headlines. 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

ONLINE CHALLENGES

Appropriately supporting discussions about online scare stories

CSAP > 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

CROSSING THE LINE

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

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. The SWGfL Project Evolve resource highlighted on page 14 above can provide an excellent basis for this aspect. In addition, good practice demonstrates that where learners are involved in contributing to 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 page 28 of this guidance provides an excellent child-centric insight that can support this approach.

Resources:

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

CEOP > ThinkUKnow (TUK) Teacher Resources
Useful TUK Teacher Resource area which can be searched by category and age
www.thinkuknow.co.uk/professionals/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

95. 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 and colleges to individually customise filtering policies according to local requirements such as by a user group or key stage and this approach 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 32-34 of this guidance.

Inspection

96. Since September 2019, Ofsted's inspections of early years, schools and post-16 provision are carried out under: Ofsted's Education Inspection Framework. Inspectors will always report on whether or not arrangements for safeguarding children and learners are effective.

97. In addition to the framework and inspections handbooks, Ofsted publishes specific guidance to inspectors on inspecting safeguarding: Inspecting safeguarding in early years, education and skills settings.

98. 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 it inspects at Independent Schools Inspectorate.

Advice

Ofsted's guidance for inspectors on inspecting safeguarding includes numerous references to online safety and it is clear there is an expectation 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 and evidence current practice to identify strengths and areas for improvement using the very-highly recommended (updated) SWGfL 360ºSafe self-review tool highlighted on page 10 of this guidance.

Resources:

Ofsted
raising standards
improving lives

Inspecting safeguarding in early years, education and skills settings

Guidance for inspectors carrying out inspections under the education inspection framework from September 2019

Ofsted > Inspecting safeguarding in early years, education and skills settings
Setting-specific guidance for Ofsted inspectors on inspecting safeguarding (September 2019)
https://www.gov.uk/government/publications/inspecting-safeguarding-in-early-years-education-and-skills

Peer on peer abuse

105. 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.

106. Governing bodies and proprietors should ensure that their child protection policy includes:

[…]

- the different forms peer on peer abuse can take, such as:
    - bullying (including cyberbullying);
    - physical abuse which can include hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm;
    - 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;
    - upskirting, which typically involves taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm;
    - sexting (also known as youth produced sexual imagery): 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
    - initiation/hazing type violence and rituals.

Advice

As referred to on page 7 of this guidance, 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 different types of peer-on-peer abuse, including Bullying, Upskirting and 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. Of particular note when there may be a need to confiscate an item (e.g. smartphone), staff should be familiar with the DfE *Searching, screening and confiscation* guidance highlighted below.

DSLs in particular should ensure they are expressly familiar with local and national guidance and recommended good practice. The UKSIC and UKCIS Managing Sexting resources highlighted under 'Safeguarding Issues' on page 6 above are excellent supporting resources to support Schools and Colleges with this aspect. Where escalation of Sexting incidents to the Police may be required (Note: see CSAP flowchart criteria advice 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)

Departmental advice for staff and school leaders explaining schools' powers of screening and searching pupils

https://www.gov.uk/government/publications/searching-screening-and-confiscation

Children with special educational needs and disabilities

126. 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 strongly recommended. Social Media can be particularly challenging for those with additional needs. Helping learners to navigate safely is a key aspect and colleagues at Internet Matters have a practical set of resources that can be useful with this. Additionally, the highly-regarded STAR Toolkit from Childnet has seen recent updates and helps to empower school staff with guidance and resources to support young people across Key Stage 2 and 3 who have special educational needs.

Resources:

Internet Matters > Connecting Safely Online
Support for parents, carers, and young people with additional learning needs. A hub of advice providing tailored information on how to connect safely online across a range of social platforms
https://www.internetmatters.org/connecting-safely-online

Childnet > STAR Toolkit (updated)
Guidance and resources to empower school colleagues with the relevant knowledge they need to support young people who have special educational needs
www.childnet.com/resources/star-sen-toolkit

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

Confidentiality

234. 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 areas related to 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 and any concerns of a confidential nature should be addressed through established mechanisms rather than via online platforms.

Useful tip: Where employed, Social Media should be used to enhance and support other forms of engagement, rather than replace them (e.g. complaints processes, parental sessions).

Part five: Child on Child Sexual Violence and Sexual Harassment

274. 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, the Safeguarding Partnership 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.
KCSIE para 281 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 73-75 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

---

> ### Action following a report of sexual violence and/or sexual harassment
>
> **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

Page 77 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.
KCSIE para 282 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 safeguarding information

Child Criminal Exploitation (CCE)

CCE is where an individual or group takes advantage of an imbalance of power to coerce, control, manipulate or deceive a child into any criminal activity (a) in exchange for something the victim needs or wants, and/or (b) for the financial or other advantage of the perpetrator or facilitator and/or (c) through violence or the threat of violence. The victim may have been criminally exploited even if the activity appears consensual. CCE does not always involve physical contact; it can also occur through the use of technology.

[…]

Child Sexual Exploitation (CSE)

CSE occurs where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child 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. CSE does not always involve physical contact; it can also occur through the use of technology. CSE 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. It can include both contact (penetrative and non-penetrative acts) and non-contact sexual activity and 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).

[…]

Advice

Annex A contains additional information about specific forms of abuse and safeguarding issues and includes the addition of a useful Table of Contents covering 18 aspects including Child Criminal Exploitation (CCE), Child Sexual Exploitation (CSE), Radicalisation, Peer-on-peer abuse, Sexual violence and harassment and Upskirting, all of which include reference to online elements.

Both the CCE and CSE sections include potential indicators of exploitation. CSE in particular 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
18-minute film and associated learning resources exploring issues of emotional and sexual abuse within teenage relationships, aimed at helping young people to recognise the signs that their relationship may be putting them at risk
www.thinkuknow.co.uk/professionals/resources/exploited

CSAP 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

ONLINE BLACKMAIL.
A ONE-HOUR LEARNING SESSION HELPING 15-18 YEAR OLDS IDENTIFY RISK AND GET SUPPORT WHEN THEY NEED IT
THINK U KNOW
PSHE Association Quality Assured Resource

CEOP > Online Blackmail Resource
A 1-hour lesson for 15-18 y/o to help identify key characteristics of how blackmail manifests online, the impact it can have and the help available
www.thinkuknow.co.uk/professionals/resources/online-blackmail

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[107] 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 or the internet) and settings (such as within the home).

[…]

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[109] to the need to prevent people from being drawn into terrorism".[110] 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, especially paragraphs 57-76, which are specifically concerned with schools (and also covers childcare). The guidance is set out in terms of four general themes: risk assessment, working in partnership, staff training, and IT policies.

Advice

This section of Annex A 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

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

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

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/

Very Highly Recommended
CSAP

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

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 (*Protecting children*) on pages 32-34 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 33 of this guidance.

Peer on peer / child on child 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): abuse within intimate partner relationships; 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.

[…]

Sexual harassment

When referring to sexual harassment we mean 'unwanted conduct of a sexual nature' that can occur online and offline. When we reference sexual harassment, we do so in the context of child on child sexual harassment. […]

Whilst not intended to be an exhaustive list, sexual harassment can include:

- sexual comments, such as: telling sexual stories, making lewd comments, making sexual remarks about clothes and appearance and calling someone sexualised names;
- sexual "jokes" or taunting;
- physical behaviour, […]
- online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence.[114] It may include:
    - non-consensual sharing of sexual images and videos;
    - sexualised online bullying;
    - unwanted sexual comments and messages, including, on social media;
    - sexual exploitation; coercion and threats; and
    - upskirting.

Advice

As is apparent from the above extracts, peer-on-peer abuse, sexual violence and sexual harassment between children include a significant number of online elements. These sections highlight that these 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. Ensuring that these are not dismissed as 'banter' will help to prevent normalisation of such behaviours and reinforce that these types of abuse will not be tolerated. The section gives useful guidance in this respect along with a variety of sources of additional advice and support mapped against each of the issues highlighted.

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

Upskirting[115]

The Voyeurism (Offences) Act, which is commonly known as the Upskirting Act, came into force on 12 April 2019. 'Upskirting' is where someone takes a picture under a persons clothing (not necessarily a skirt) without their permission and or knowledge, with the intention of viewing their genitals or buttocks (with or without underwear) to obtain sexual gratification, or cause the victim humiliation, distress or alarm. It is a criminal offence. Anyone of any gender, can be a victim.

Advice

The section on Upskirting, originally introduced in 2019, has seen amendment for 2020, now making explicit reference to The Voyeurism (Offences) Act. *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 England and Wales in April 2019 punishable by up to 2 years in prison with the most serious offenders being placed on the Sex Offenders Register. The Ministry of Justice have produced a useful guide explaining Upskirting, including the background, legislation and where to get support.

Resources:

GOV.UK

Ministry of Justice

Upskirting: know your rights

HM Govt > Upskirting: Know your rights

Useful guidance from the Ministry of Justice explaining what 'Upskirting' is, what the law says and where to get help

https://www.gov.uk/government/news/upskirting-know-your-rights

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.[116] The designated safeguarding lead should take **lead responsibility** for safeguarding and child protection (including online safety). This should be explicit in the role holder's job description. […]

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 and Senior Mental Health Leads) on matters of safety and safeguarding (including online and digital safety) and when deciding whether to make a referral by liaising with relevant agencies; and
- act as a source of support, advice and expertise for all staff.

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. Training should provide designated safeguarding leads with a good understanding of their own role, and the processes, procedures and responsibilities of other agencies, particularly children's social care, 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;
> - obtain access to resources and attend any relevant or refresher training courses; and
> - 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.
>
> In addition to the formal training set out above, their knowledge and skills should be refreshed (this might be via e-bulletins, meeting other designated safeguarding leads, or simply taking time to read and digest safeguarding developments) at regular intervals, as required, and at least annually, to allow them to understand and keep up with any developments relevant to their role.

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 Assurance Partnership 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:

CSAP & UKSIC > Online Safety Live (in Lancashire) Briefing Sessions
Extremely popular, very highly-recommended 2-hour events held in January each year, hosted by the Children's Safeguarding Assurance Partnership and delivered by 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. The resulting summary animation provides invaluable information and can be used to help inform staff awareness sessions as well as providing 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

CSAP > 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 Children's Safeguarding Assurance Partnership 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 Partnership has a dedicated Learning & Development Team which incorporates an array of wider safeguarding-related resources and courses relevant to DSLs, including the highly-popular 7-Minute Briefings covering a wide range of safeguarding topics.

Resources:

CSAP
Online
Safeguarding
Dedicated website section to support Teachers & Professionals
Children's Safeguarding Assurance Partnership
working together to stay safe online

CSAP > Lancashire Online Safeguarding Web pages
Dedicated online safety section to support colleagues in schools, colleges and the wider children's workforce
www.lancashiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce

CSAP > Learning & Development
Useful wide range of safeguarding courses and learning resources for staff including online safety and the very popular 7-Minute Briefing series
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 received a number of revisions for 2020 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 a useful means of categorising risk areas according to type. In addition, a fourth risk area is sometimes used to include 'Commercial' - referring to risks around financial or data-related issues (e.g. harvesting of personal information for financial purposes). It is important to recognise that these risk areas are not mutually exclusive (e.g. extremist content can also apply to 'Conduct' as well as 'Content').

As is apparent, the range of online safety issues is broad and often complex, with terminology continually developing. To support this, the Safeguarding Partnership has developed *the little BIG book of Online Safety terms* which helps to explain some common terms associated with the online environment and can be particularly useful for those new to online safety.

Resources:

The little BIG book of Online Safety terms

An A-Z collection of common Online Safety terminology explained

Children's Safeguarding Assurance Partnership

working together to stay safe online

CSAP > Little BIG Book of Online Safety Terms (3rd edition)
An A-Z glossary of Online Safety terminology referencing over 200 terms commonly used in Online Safety
www.lancashiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce#Glossary

Education

Opportunities to teach safeguarding, including online safety, are discussed at paragraph 93-95. Resources that could support schools and colleges include:

- **Be Internet Legends** developed by Parent Zone and Google is a free internet safety curriculum with PSHE accredited lesson plans and teaching resources for Key Stage 2 pupils
- **Disrespectnobody** is Home Office advice and includes resources on healthy relationships, including sexting and pornography
- **Education for a connected world framework** from the UK Council for Internet Safety supports the development of the curriculum and is of particular relevance to RSHE education and Computing. It is designed, however, to be usable across the curriculum and beyond (covering early years through to age 18) and to be central to a whole school or college approach to safeguarding and online safety.
- **PSHE association** provides guidance to schools on developing their PSHE curriculum
- **Teaching online safety in school** is departmental guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements
- **Thinkuknow** is the National Crime Agency/CEOPs education programme with age specific resources
- **UK Safer Internet Centre** developed guidance and resources that can help with the teaching of the online safety component of the Computing Curriculum.

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, up-to-date and empower them to be able to respond to a range of online threats as well as opportunities.

This section, first introduced in 2018, builds upon the information in paras 93-95 (*Opportunities to teach safeguarding*) and highlights a number of very useful resources. The 2020 update includes reference to the Disrespectnobody resources from the Home Office, which include resources on Sexting, Relationship Abuse and Consent.

As in recent years, of particular note is the reference to the UKCIS framework *'Education for a Connected World'* (EFACW) originally highlighted on Page 14 of this resource. This resource has seen an update in 2020 and continues to be highly-recommended and extremely useful when planning curriculum delivery that is both age-appropriate and progressive.

Related to the UKCIS framework and further supporting Online Safety education, colleagues at SWGfL have developed Project EVOLVE. Project EVOLVE includes resources referencing each of the 300+ statements in the UKCIS EFACW framework. The toolkit includes research; activities; outcomes; supporting resources and professional development materials to support effective online safety progression and is **very highly recommended as an essential toolkit resource for Schools and Colleges** across the region when addressing Online Safety.

Resources:

SWGfL > Project EVOLVE

An excellent and very highly-regarded suite of (freely-available) progressive resources and activities to support online safety education and implementing the EFACW framework statements.

https://projectevolve.co.uk/

Very Highly Recommended

CSAP

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

Education for a Connected World

A framework to equip children and young people for digital life

UK Council for Internet Safety

2020 edition

Very Highly Recommended

CSAP

UKCIS > Education for a Connected World (2020 edition)
Excellent & very highly-recommended progressive framework set across 8 online safety strands, highlighting levels for Early Years – 7; 7 – 11; 11 – 14 and 14 – 18 y/o.
www.gov.uk/government/publications/education-for-a-connected-world

SWGfL

Education that Clicks

Swiggle

CHILD FRIENDLY SEARCH

Very Highly Recommended

CSAP

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 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 from September 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

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

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

> ### Protecting children
>
> 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.[119] 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

In previous revisions, this section had a title of *Filters and monitoring* although the content remains intact. 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, 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 potential services.

Schools may also wish to approach their provider/s to consider the range of features 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:

UKSIC > Appropriate **Filtering** Guidance (June 2020)
Useful guidance for education settings on establishing appropriate levels of filtering
https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering

UKSIC > Appropriate **Monitoring** Guidance (June 2020)
Useful guidance on establishing appropriate levels of monitoring
https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring

Advice

It is important to recognise and understand 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 freely-available 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 24 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.

Useful tip: When using the Filter Check utility, save a screen grab of the results and include a dated copy with the School/College's Online Safety Policy as evidence of checking filtering compliance.

Resources:

SWGfL > Internet Filter Test for Schools
Freely-available content filter test 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 regard 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.

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 to help responsible bodies assure themselves that their online safety arraignments are effective.

Advice

Experience shows that whilst there is typically focus on Policies/Procedures and Technology/Education, the associated emphasis on reviewing the effectiveness of provision can sometimes be overlooked. As referred to on page 10 of this guidance, the 360° Safe v2.0 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 has been updated in 2020 and 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 Safeguarding Partnership has developed a CSAP 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 has been updated in 2020 and identifies a number of ‘inward’ and ‘outward’ facing questions to support ensuring effective provision.

Resources:

Online Safety Governance Checklist

☑ Review Guidance to support Governors & Proprietors

Children's Safeguarding Assurance Partnership
working together to stay safe online

CSAP > Governor Online Safety Self-Review Tool (Updated Sept 2020)
CSAP prompts to support Governors & Proprietors when review Online Safety provision in their settings
www.lancashiresafeguarding.org.uk/online-safeguarding/schools-the-childrens-workforce#GovernorSRT

Education at home

Where children are being asked to learn online at home the department has provided advice to support schools and colleges do so safely: safeguarding-in-schools-colleges-and-other-providers and safeguarding-and-remote-education

Advice

This new addition for 2020 highlights safeguarding considerations where children are learning at home. Without the usual structure of physically attending school, opportunities to identify safeguarding concerns for both children and staff may be more challenging. Within the new statement are links to DfE guidance which emphasises the need to reinforce the importance of children staying safe online to parents and carers.

Considerations to support learning at home and its practical application have understandably increased substantially in comparison to previous years. Colleagues at SWGfL have produced a variety of very useful guidance to support schools and colleges with remote learning. Relatedly, this includes a useful checklist and advice for the appointment of external tutors to deliver online education as an area requiring careful safeguarding consideration.

A large range of Online Safety-related activities for learners to do at home can be found through CEOP's Think You Know (TUK) programme. These include a number of home activity packs covering both Primary and Secondary age learners and their Parents/Carers across a variety of topics.

Resources:

SWGfL Safe, Secure, Online

Safe Remote Learning

Considerations to safeguard remote learning

Download Flyer

SWGfL > Safe Remote Learning

Useful information to support schools organising remote online learning, including policies, platforms, education, behaviours and safeguarding considerations

https://swgfl.org.uk/resources/safe-remote-learning/

SWGfL Safe, Secure, Online

Choosing Online Tutors for your School

Download Overview

SWGfL > Choosing Online Tutors for your School

Useful checklists and advice when considering the appointment of external tutors to deliver education online

https://swgfl.org.uk/resources/safe-remote-learning/online-tutoring

THINK U KNOW .co.uk

Home Activity Packs

Learning about online safety at home

CEOP TUK > Home Activity Packs

A large library of clips, activities, games and challenges to support learners and their parents/carers

https://www.thinkuknow.co.uk/parents/support-tools/home-activity-worksheets

Staff training

Governors and proprietors should ensure that, as part of the requirement for staff to undergo regularly updated safeguarding training (paragraph 89) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 93), 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 an **integral part** of their overarching 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, such as attending the Online Safety Live in Lancashire sessions highlighted on page 27 of this guidance.

Useful tip: Whilst they will understandably 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 existing 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 15 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, it is recommended good practice to ensure that 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 CSAP website in both the Learning & Development and dedicated Online Safeguarding sections.

Resources:

Children's Safeguarding Assurance Partnership

7 Minute Briefings

Social Media & Mental Health

CSAP > 7-Minute Briefing (Social Media & Mental Health)
Useful short, summary snapshot looking at Social Media and Mental Health & Wellbeing
www.lancashiresafeguarding.org.uk/learning-development/7-minute-briefings

Children's Safeguarding Assurance Partnership

Learning & Development Course Event

Safer Online Behaviours (Children)

CSAP > Learning & Development Courses and Events
Information about the variety of training events provided through the CSAP 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/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

Advice for governing bodies/proprietors and senior leaders

- Childnet provide guidance for schools on cyberbullying

[…]

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other

[…]

Support for children

- Childline for free and confidential advice

[…]

Parental support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support

[…]

Advice

This section of Annex C sees a substantial revision to previous versions with a variety of signposts added to useful resources under related headings as can be seen above. One of the challenges most often 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 previously mentioned 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 and the Project EVOLVE toolkit highlighted on page 14 of this guidance is extremely useful in this regard.

Along with those resources highlighted within this *Making Sense of…* guidance, the Safeguarding Partnership'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:

CSAP
Online
Safeguarding
Dedicated website section to support Teachers & Professionals
Children's Safeguarding Assurance Partnership
working together to stay safe online

CSAP > Lancashire Online Safeguarding Web pages

Dedicated online safety section to support colleagues in schools, colleges and the wider children's workforce

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

CSAP > Twitter

Lancashire Safeguarding Twitter account providing Safeguarding related news and updates including Online Safety

https://twitter.com/LancsSguarding

Summary

As will be apparent, the Online Safeguarding agenda continues to evolve significantly 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 CSAP 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
CSAP/LSAB Online Safeguarding Advisor
Chair, Pan-Lancashire Online Safeguarding Group
Children's Safeguarding Assurance Partnership
September 2020

e-mail: graham.lowe2@lancashire.gov.uk
web: www.lancashiresafeguarding.org.uk
twitter: @LancsSguarding

Children's
Safeguarding Assurance
Partnership
working together to stay safe online

Concerns about a child should be reported on 0300 123 6720 or out of hours 0300 123 6722 (5pm - 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 Safety is available from the CSAP Online Safeguarding homepage at: www.lancashiresafeguarding.org.uk/online-safeguarding

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 2020. Advice has been referenced from a variety of Pan-Lancashire school colleagues, governors and wider organisations, working together to collate useful recommendations and experience of good practice.