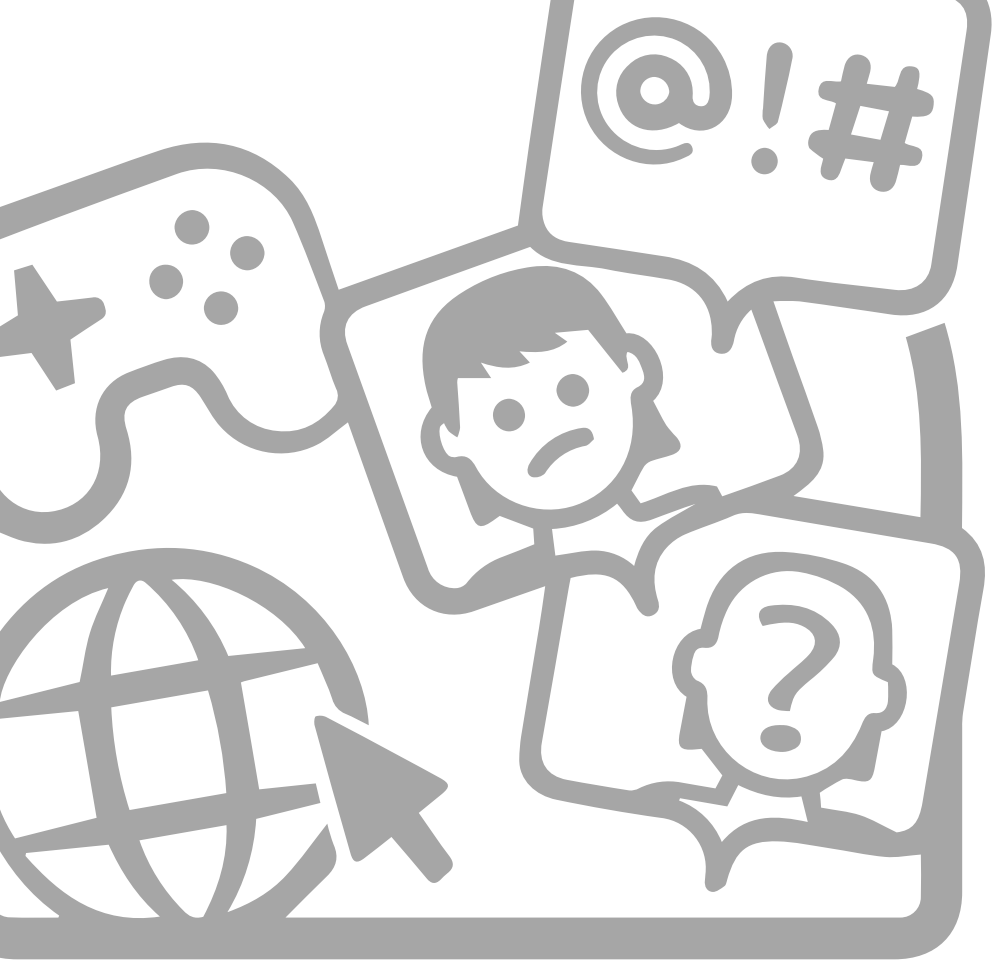


Making Sense of...

Keeping children safe in education 2021

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 five : rev4621 :
November 2021

Children's Safeguarding Assurance Partnership
Blackburn with Darwen - Blackpool - Lancashire

*Making Sense of...*Keeping Children Safe in Education

Content Quick Links

*Making Sense of…*Keeping Children Safe in Education 2021

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 has since been updated annually, 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 2021, 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 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
Children's Safeguarding Assurance Partnership
September 2021

e-mail: graham.lowe2@lancashire.gov.uk
web: www.safeguardingpartnership.org.uk
twitter: @CSAP_LSAB

Children's Safeguarding Assurance Partnership
Blackburn with Darwen - Blackpool - Lancashire

Making Sense of…KCSIE: Legend

123. **Example KCSIE extract**: a direct reference from the text within Keeping children safe in education (KCSIE) 2021. 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:

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.safeguardingpartnership.org.uk

Part one: Safeguarding information for all staff

Abuse and neglect

22. **All** school and college staff should be aware that abuse, neglect and safeguarding issues are rarely standalone events and cannot be covered by one definition or one label alone. In most cases, multiple issues will overlap with one another, therefore staff should always be vigilant and always raise any concerns with their designated safeguarding lead (or deputy).
[…]
24. **All** staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.

26. **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.

28. **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, or the exploitation or corruption of children. Some level of emotional abuse is involved in all types of maltreatment of a child, although it may occur alone.

Advice:

Para 24 is a new addition for KCSIE 2021 and emphasises the role technology can play in safeguarding and wellbeing issues. Importantly, this paragraph highlights that different forms of abuse often take place concurrently, both online and offline and that children can also abuse other children. Para 28 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

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 International

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 17 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.

29. **Sexual abuse:** involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving 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 (also known as peer on peer abuse) in education and all staff should be aware of it and of their school or colleges policy and procedures for dealing with it, (see paragraph 49).

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 sharing nude/semi-nude images and/or videos). This clearly identifies that Schools and Colleges must include the online aspects when addressing Child Sexual Exploitation (CSE) and ensure that Safeguarding and Child Protection policies and procedures cover online sexual abuse. Peer-on-peer abuse is further referenced on pages 9, 26 & 30 of this guidance.

Safeguarding issues

31. 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 and or alcohol misuse, deliberately missing education and consensual and non-consensual sharing of nudes and semi-nudes images and/or videos[9] can be signs that children are at risk. Other safeguarding issues all staff should be aware of include:

[9] Consensual image sharing, especially between older children of the same age, may require a different response. It might not be abusive – but children still need to know it is illegal - whilst non-consensual is illegal and abusive. UKCIS provides detailed advice about sharing of nudes and semi-nude images and videos.

Child Sexual Exploitation (CSE)

36. CSE is a form of child sexual abuse. Sexual abuse may involve physical contact, including assault by penetration (for example, rape or oral sex) or nonpenetrative acts such as masturbation, kissing, rubbing, and touching outside clothing. It may include non-contact activities, such as involving children in the production of sexual images, forcing children to look at sexual images or watch sexual activities, encouraging children to behave in sexually inappropriate ways or grooming a child in preparation for abuse including via the internet.

37. CSE can occur over time or be a one-off occurrence, and may happen without the child's immediate knowledge e.g. through others sharing videos or images of them on social media.

Advice:

All members of staff must be aware of a range of safeguarding issues and these paragraphs specifically highlight the need for staff to be aware of consensual and non-consensual sharing of nude and semi-nude images and/or videos (previously referred to as 'Sexting')[1] and Child Sexual Exploitation.

[1] It is important to carefully consider the terminology we use and its inferred associations, particularly when referring to non-consensual sharing of nude/semi-nude images and/or videos. Such non-consensual sharing by children and young people should not be referred to as 'Revenge Porn' (a term typically associated with intimate image abuse relating to adults). The CSAP/LSAB *'little BIG book of Online Safety Terms'* highlighted below can be a useful reference where colleagues may be unsure about different terminology.

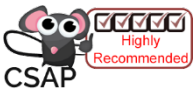
Although it may be viewed by young people as a 'mundane' activity or 'normal flirtatious behaviour', by taking and sending an explicit image (even if the picture is taken/shared with their permission), a young person is producing and distributing an indecent image of a child and risks being prosecuted. This may be an indicator of other safeguarding issues and also increases the risk of sexual exploitation, bullying and/or blackmail as well as being a significant source of emotional distress and unwanted attention. Such 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.

CSE may involve utilising the Internet and social media to identify potential victims or as a tool to coerce or blackmail children into performing sexual acts, both online and offline. Means of accessing the Internet may also be provided to the child or young person as a "gift" by perpetrators such as in the form of new mobile phones and devices. In some cases, CSE can take place entirely online such as children being coerced into performing sexual acts via webcam/social media and therefore may not always result in a physical meeting between children and the offender. DSLs should be aware of National and Local policy and procedures regarding CSE and ensure that school-based policies relating to CSE explicitly include reference to online aspects. Further additional information about Child Sexual Exploitation is included on pages 127 & 128 in Annex B of KCSIE and includes definitions and potential indicators.

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

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



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

UKCIS > Sharing nudes and semi-nudes (new)
Comprehensive advice for education settings outlining how to manage and respond to incidents of nudes and semi-nudes being shared
https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

CSAP/LSAB > The little BIG book of Online Safety Terms (updated November 2021)
An A-Z collection of common Online Safety terminology explained
https://www.safeguardingpartnership.org.uk/online/resources/#CSAPResources

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:

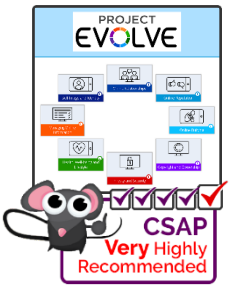
The sharing of nude and semi-nude images and/or videos is an issue which should be highlighted within staff safeguarding training. Designated Safeguarding Leads (DSLs) should also take action to ensure that all members of staff are explicitly clear about how to respond to such concerns appropriately and in line with the school/college policy (e.g. all members of staff should be aware that if a child discloses they have sent or received a "nude", then these images should not be printed, copied or forwarded). In those circumstances where further escalation may be required (e.g. Police referral), it is important that this should follow established safeguarding procedures via the Designated Safeguarding Lead. Section 2.3 (Initial Review Meeting) of the UKCIS guidance *'Sharing nudes and semi-nudes: advice for education settings working with children and young people'* contains comprehensive guidance and identifies 5 criteria on page 20 which may require a referral via the MASH to the Police and/or Children's Social Care to be made.

Relatedly, the UK Safer Internet Centre has produced some useful summary guidance on appropriately responding to and managing Sexting incidents and the highly-recommended Project EVOLVE toolkit from SWGfL provides a range of age-appropriate learning resources under its Online Relationships strand.

Note: It is strongly recommended that all DSLs should be expressly familiar with the UKCIS guidance *'Sharing nudes and semi-nudes: advice for education settings working with children and young people'*.

Resources:

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



(new) SWGfL > Project EVOLVE (Online Relationships strand)
A large array of classroom resources mapped against the Education for a Connected World (EFACW) framework to be used across a variety of ages to explore relationships including respect, consent and behaviours that may lead to harms
https://projectevolve.co.uk/toolkit/

Advice:

Whilst we may understandably take a preventative approach towards the sharing of nude/semi-nude images and videos, post-incident advice to support young people experiencing issues resulting from such activity is essential. The South West Grid for Learning (SWGfL) have a very useful (freely available) resource *"So you got naked online..."* which provides practical advice and information for Young People experiencing issues. In addition, a further version has been developed to provide accessible information to help support young people (KS3+) with particular vulnerabilities.

Resources:

SWGfL > So you got naked online...
Useful supporting resource offering children, young people and parents advice to support the issues resulting from the sharing of nudes/semi-nudes
https://swgfl.org.uk/resources/so-you-got-naked-online

(new) SWGfL/Internet Matters > So you got naked online... (SEND)
Useful supporting resource offering young people with particular vulnerabilities advice to support the issues resulting from sharing of nudes/semi-nudes
https://www.internetmatters.org/hub/resource/so-you-got-naked-online-send-version

---

Mental Health

41. All staff should 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.

[…]

44. Schools and colleges can access a range of advice to help them identify children in need of extra mental health support, this includes working with external agencies. More information can be found in the mental health and behaviour in schools guidance, colleges may also wish to follow this guidance as best practice. Public Health England has produced a range of resources to support secondary school teachers to promote positive health, wellbeing and resilience among children. See Rise Above for links to all materials and lesson plans.

Advice:

As well as being a potential indicator of abuse, neglect, exploitation or other Adverse Childhood Experiences (ACEs), it is clear that 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 resources highlighted in the text 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 > Every Mind Matters
Lesson plans and resources from Public Health England supporting a wide variety of aspects affecting physical and mental wellbeing
https://campaignresources.phe.gov.uk/schools/topics/mental-wellbeing/overview

Peer on peer abuse (child on child)

46. **All** staff should be aware that children can abuse other children (often referred to as peer on peer abuse). And that it can happen both inside and outside of school or college and online. It is important that all staff recognise the indicators and signs of peer on peer abuse and know how to identify it and respond to reports.
[…]

49. Peer on peer abuse is most likely to include, but may not be limited to:

- bullying (including cyberbullying, prejudice-based and discriminatory bullying);
- abuse in intimate personal relationships between peers;
- physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm (this may include an online element which facilitates, threatens and/or encourages physical abuse);
- sexual violence,[11] such as rape, assault by penetration and sexual assault; (this may include an online element which facilitates, threatens and/or encourages sexual violence);
- sexual harassment,[12] such as sexual comments, remarks, jokes and online sexual harassment, which may be standalone or part of a broader pattern of abuse;
- causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party;
- consensual and non-consensual sharing of nudes and semi nudes images and or videos[13] (also known as sexting or youth produced sexual imagery);
- upskirting,[14] which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm; and
- initiation/hazing type violence and rituals (this could include activities involving harassment, abuse or humiliation used as a way of initiating a person into a group and may also include an online element).

Advice:

As is apparent above, online elements can form a significant part of peer on peer abuse and has seen the inclusion of additional aspects for 2021. ALL members of staff should therefore understand that abuse can also be perpetrated by children and young people themselves and may include cyberbullying (Online Bullying), upskirting and the sharing of nude/semi-nude images. In addition, staff should be aware that pressure to participate in 'online challenges' shared via social media can be a significant source of concern for young people. 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 B of KCSIE 2021 provides further additional details on these and other forms of abuse and is referred to in greater detail on pages 26 & 29 of this guidance.

Part two: The management of safeguarding

The responsibility of governing bodies, proprietors and management committees

Safeguarding policies and procedures

84. 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.

85. These policies should include individual schools and colleges having:

- an effective **child protection policy** which:
  - reflects the whole school/college approach to peer on peer abuse (see para 145);
  - reflects reporting systems as set out at paragraph 83;
  - should describe procedures which are in accordance with government guidance;
  - refers to locally agreed multi-agency safeguarding arrangements put in place by the safeguarding partners;
  - includes policies as reflected elsewhere in Part two of this guidance, such as online safety (see paragraph 126), and special educational needs and disabilities (SEND) (see paragraphs 185-187);
  - where appropriate, reflects serious violence. Further advice for schools and colleges is provided in the Home Office's Preventing youth violence and gang involvement and its Criminal exploitation of children and vulnerable adults: county lines guidance;
  - should be reviewed annually (as a minimum) and updated if needed, so that it is kept up to date with safeguarding issues as they emerge and evolve, including lessons learnt; and
  - is available publicly either via the school or college website or by other means.
- a **behaviour policy**[23], which includes measures to prevent bullying (including cyberbullying, prejudice-based and discriminatory bullying)
- a **staff behaviour policy** (sometimes called the code of conduct) which should, amongst other things, include: acceptable use of technologies (including the use of mobile devices), staff/pupil relationships and communications including the use of social media.[24]
- **appropriate safeguarding arrangements** in place to respond to children who go missing from education, particularly on repeat occasions (more information at paragraph 164).

86. The above is not intended to be an exhaustive list. These policies and procedures, along with Part one (or Annex A if appropriate) of this guidance and information regarding the role and identity of the designated safeguarding lead (and deputies), should be provided to all staff on induction.

Advice:

The emphasis on the responsibilities of Governing bodies/proprietors continues to be explicitly evident throughout KCSIE and has multiple specific references to aspects relating to the online environment. Understanding these 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. Whilst specific arrangements should be made to suit local circumstance, it is viewed as good practice to include Governor colleagues when arranging Online Safety training for school staff wherever possible. To further support Governor colleagues, the Safeguarding Partnership has developed and updated a local summary self-review checklist resource to aid Governors as part of their approach to addressing online safety provision.

Resources:

CSAP > Online Safety Governance Checklist: (updated Sept 2021)
Locally-developed Governor self-assessment checklist to support with reviewing school/college online safety provision
https://www.safeguardingpartnership.org.uk/online/resources/#CSAPResources

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

Advice:

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

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

Given the pace at which the online world continues to develop, experience shows that minor updates to outdated 'e-Safety' policies presents a risk in failing to address the current issues faced by schools and importantly, today's challenges faced by pupils/students. As such, a question 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 utilise 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 benchmark, 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 > 360° 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

89. 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 (including online safety). This should be explicit in the role-holder's job description (see Annex C, which describes the broad areas of responsibility and activities related to the role).

Advice:

Online Safety is primarily a Safeguarding issue and (updated for 2021), now explicitly references that the responsibility for Online Safety falls within the remit of the Designated Safeguarding Lead (DSL).

However, effectively addressing Online Safety requires a collaborative, whole-school approach. Therefore, staff with appropriate skills, interest and expertise should be encouraged to help support the DSL(s) as appropriate, for example when developing curriculum approaches or making technical decisions. 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 (rather than ICT) issue.

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

94. 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.

95. 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 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 95, 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. Equally, the safeguarding partnership makes positive use of social media through its Twitter presence, regularly providing specific updates relating to Online Safety, including useful signposts to current developments.

More formally, this may include CPD opportunities recommended through the Safeguarding Partnership arrangements such as those from the relevant Local Authority or other reputable external providers. Further information on these aspects including the annual Online Safety Live in Lancashire sessions can be found on pages 14 & 41 of this guidance.

Resources:

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

Staff training

114. 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 safeguarding partners.

115. In addition, all staff should receive regular safeguarding and child protection updates, including online safety (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.
[…]

117. Governing bodies and proprietors should ensure that, as part of the requirement for staff to undergo regular updated safeguarding training, including online safety (paragraph 114) and the requirement to ensure children are taught about safeguarding, including online safety (paragraph 119), that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning.

Advice:

It is clear that reference to online safety is increasingly prominent when relating to staff training. However, research regularly informs us that staff training is typically the weakest area of provision when assessing Online Safety practice. 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 40-41 of this guidance. Regular updates may include using the highly-popular CSAP 7-Minute Briefing resources (which include online safety-related topics) or by attending specific Online Safety sessions such as those offered through the Safeguarding Partnership.

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
https://www.safeguardingpartnership.org.uk/learn

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.

Relatedly, staff should be involved in the development of the Online Safety Policy and related procedures to promote ownership, understanding and developing their own professional knowledge. This may include involving staff in development via discussions at staff meetings or reviewing policies with staff working groups. Additionally, it is strongly recommended that pupils/students are also engaged to ensure that staff knowledge, and thereby the broader School/College provision, is appropriately informed by those areas of

Online Safety that may be of concern to our children and young people. This aspect is referred to in more detail on page 40 of this guidance.

The Children's Safeguarding Assurance Partnership (CSAP) in partnership with UKSIC colleagues have provided free-of-charge annual updates for a number of years 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), update on current aspects and trends around Online Safety. Attendance at the events also provides attendees with the opportunity to cascade content and the insights gained to other members of staff in school.

Note: Designated Safeguarding Leads in particular are strongly advised to attend one of the available Online Safety Live 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
https://www.safeguardingpartnership.org.uk/online/#OS_NewsEvents

---

Opportunities to teach safeguarding

119. Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety, and recognise that a one size fits all approach may not be appropriate for all children, and a more personalised or contextualised approach for more vulnerable children, victims of abuse and some SEND children might be needed.
[…]

121. The Department has produced a one-stop page for teachers on GOV.UK, which can be accessed here: Teaching about relationships sex and health. This includes teacher training modules on the RSHE topics and non-statutory implementation guidance. The following resources may also help schools and colleges understand and teach about safeguarding:

- DfE advice for schools: teaching online safety in schools;
- UK Council for Internet Safety (UKCIS)[32] guidance: Education for a connected world;
- UKCIS guidance: Sharing nudes and semi-nudes: advice for education settings working with children and young people;
- The UKCIS external visitors guidance will help schools and colleges to ensure the maximum impact of any online safety sessions delivered by external visitors;
- 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 across 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 results in messages being viewed as irrelevant, outdated or not-in-touch with current challenges and therefore will lead to disengagement by pupils/students.

Good practice demonstrates that questioning pupils/students on their concerns helps to inform an evidence-based approach 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.

Addressing this challenge, the UK Council for Internet Safety (UKCIS) provides the extremely useful and very highly recommended Education for a Connected World (EFACW) framework which can provide much-needed structure and importantly, currency and progression across a number of related online themes.

Resources:

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 informs us that delivering those statements identified in the framework can sometimes be a challenge - therefore, the Safeguarding Partnership strongly recommends schools and colleges make use of the freely-available Project EVOLVE Toolkit from the South West Grid for Learning (SWGfL). 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.

Note: Project EVOLVE has recently launched a new 'Knowledge Map' feature which allows staff to assess (baseline) pupil's current knowledge, plan teaching progression and then evaluate what impact it has had.

Resources:

SWGfL > Project Evolve Toolkit
A very highly-recommended (freely-available) toolkit mapped against the EFACW statements to support the delivery of age-appropriate and progressive 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 guests 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 developing 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'. As highlighted in KCSIE para 121, 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

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

CSAP > Online Challenges – Letter Template (updated November 2021)
A useful template letter which can be adapted and used to address viral scare stories/online challenges with parents and carers
https://www.safeguardingpartnership.org.uk/online/resources/#CSAPResources

Advice

Experience shows us that effective Online Safety education is 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).

However, 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, how they will address and developing their own online behaviour.

Resources:

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

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 15 above can provide an excellent basis to support schools in these aspects. 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.

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

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

UKCIS > Digital Resilience Framework
A useful summary framework to support self-assessment and decision making when considering how digital resilience is approached

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831217/UKCIS_Digital_Resilience_Framework.pdf

122. 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 tools, resources and recommended good practice around filtering and monitoring aspects are included on pages 22 & 23 of this guidance.

Online safety

123. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

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

- **content**: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact**: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.
- **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

125. Schools and colleges should ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement.

Advice:

Keeping Children Safe in Education 2021 sees a significant change for Online Safety from previous iterations (whilst reference was previously included throughout, further specific Online Safety detail was contained as a dedicated Annex).

In a substantial change for KCSIE 2021, Online Safety has been moved into the main body of the statutory guidance with subsections including: categories of risk; online safety policy; remote learning; filters & monitoring; information security and reviewing online safety. This move clearly reflects the importance of Online Safety and that it is considered to be an integral aspect of modern safeguarding arrangements for our children and young people.

The original '3C's Risk Matrix' was identified through the LSE 'EU Kids Online' project and has been a useful means of categorising risk areas according to type for a number of years. However, to reflect the evolving nature of the online environment, KCSIE 2021 sees the addition of a widely-acknowledged fourth risk area relating to 'Commerce'. This addition refers to risks around financial or data-related issues (e.g. online gambling, harvesting of personal information for financial purposes) and is also particularly relevant to the online gaming world where issues such as 'loot boxes' and 'skin trading' can have a financial impact.

Note: Whilst the categorisation of risk is a useful means of discretely identifying online risks, it is important to recognise that these risk areas are not mutually exclusive (e.g. extremism risks can apply to 'Conduct' as well as 'Content' risk areas).

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 is regularly updated and helps to explain some common terms associated with the online environment and can be particularly useful for those new to online safety.

Resources:

CSAP > Little BIG Book of Online Safety Terms (updated November 2021)
A regularly updated A-Z glossary of Online Safety terminology referencing over 200 terms commonly used in Online Safety
https://www.safeguardingpartnership.org.uk/online/resources/#CSAPResources

Online safety policy

126. Online safety and the school or college's approach to it should be reflected in the child protection policy. Considering the 4Cs (above) will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass their peers via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect in their mobile and smart technology policy and their child protection policy.

KCSIE 2021 also sees the addition of a specific section around the Online Safety Policy. Whilst all school online safety policies should have common elements such as those referenced in KCSIE para 126, it is important that the policy reflects local arrangements and as with the broader Child Protection Policy, should be regularly reviewed to ensure currency and effectiveness - a particularly important aspect given the continually-evolving nature of the online world.
Our colleagues at the South West Grid for Learning have an excellent set of comprehensive and freely-available Online Safety Policy templates. The templates are highly recommended and include guidance, planning tools, process maps and a range of appendices to cover numerous policy-related aspects.

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 > 360° 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/

Remote learning

127. 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. The NSPCC and PSHE Association also provide helpful advice:

- NSPCC Learning - Undertaking remote teaching safely during school closures
- PSHE - PSHE Association coronavirus hub

Advice

The impact of the global Coronavirus pandemic has understandably brought renewed focus to the importance of safeguarding when 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 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 and as such, the Safeguarding Partnership has published Safer Remote Learning guidance which includes a number of prompts and considerations when providing remote learning opportunities. Colleagues at SWGfL have also 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.

In addition, 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:

CSAP > Safer Remote Learning
Considerations, prompts and recommended resources to support remote learning activity
https://www.safeguardingpartnership.org.uk/online/resources/#CSAPResources

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 > 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

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

Filters and monitoring

128. 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 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. Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs vs risks.

129. 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.[33] 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.

130. Support for schools when considering what to buy and how to buy it is available via the: schools' buying strategy with specific advice on procurement here: buying for schools.

Advice

Content filtering tools have become increasingly sophisticated and as such, a one-size-fits-all approach to content filtering across the whole school or college 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, 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. For example, the school's filtering provision may be complemented for younger learners by making use of tools such as the Swiggle search function across school devices.

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 and 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:

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/

UKSIC > Appropriate Filtering Guidance (June 2021)
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 2021)
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'.

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 Test utility, save a screen grab of the results and include a dated copy with the School/College's Online Safety Policy to evidence 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

Advice

As previously highlighted, 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.

Note: Whilst not required in all settings, where monitoring software is employed, effective practice includes ensuring reports are sent to the Safeguarding lead (as opposed to the ICT lead) as this helps to ensure potentially wider safeguarding concerns (i.e. non-ICT related) are considered. Additionally, local assessments may highlight a higher level of concerns for particular students where an enhanced level of monitoring may be required.

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 tools, children or staff can potentially bypass systems 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.

Information security and access management

131. Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place, in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. Guidance on e-security is available from the National Education Network. In addition, broader guidance on cyber security including considerations for governors and trustees can be found at NCSC.GOV.UK.

Reviewing online safety

132. Technology, and risks and harms related to it evolve and changes rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. A free online safety self-review tool for schools can be found via the 360 safe website.

133. UKCIS has published Online safety in schools and colleges: Questions from the governing board. The questions can be used to gain a basic understanding of the current approach to keeping children safe online; learn how to improve this approach where appropriate; and find out about tools which can be used to improve the approach. It has also published an Online Safety Audit Tool which helps mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring.

134. When reviewing online safety provision, the UKCIS external visitors guidance highlights a range of resources which can support educational settings to develop a whole school approach towards online safety.

Information and support

135. There is a wealth of additional information available to support schools, colleges and parents to keep children safe online. A sample is provided at Annex D.

Advice

Information security and access management is a new addition for 2021 and reflects that schools and colleges are regular targets for cyber-crime. The National Cyber Security Centre (NCSC) website has a very useful dedicated section for schools and includes a variety of resources to help improve cyber resilience, including a freely-available training package for staff and supporting videos.

The section on Reviewing Online Safety sees an expanded focus over previous years with a number of supporting resources identified and a recommendation to conduct an annual review of online safety.

Experience shows that whilst there is typically focus on Policies/Procedures and Technology/Education, the associated '*So What…*' emphasis on reviewing the effectiveness of provision is not always reflective of its critical importance.
As referred to on page 11 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 updated in 2020, 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 referred to on page 11. Again, very popular both within and outside of the Lancashire region, the CSAP Self-Review Tool has been updated for 2021 and identifies a number of 'inward' and 'outward' facing questions to support ensuring effective provision.

Resources:

NCSC > Cyber Security for Schools
Practical advice and downloadable resources to support schools and improve cyber security
https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools

CSAP > Governor Online Safety Self-Review Tool (Updated Sept 2021)
CSAP prompts to support Governors & Proprietors when review Online Safety provision in their settings
https://www.safeguardingpartnership.org.uk/online/resources/#CSAPResources

Inspection

136. 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.

137. 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.

138. 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 360°Safe self-review tool highlighted on page 11 of this guidance.

Resources:

Ofsted > Inspecting safeguarding in early years, education and skills settings
Setting-specific guidance for Ofsted inspectors on inspecting safeguarding (updated August 2021)
https://www.gov.uk/government/publications/inspecting-safeguarding-in-early-years-education-and-skills

---

Peer on peer / child on child abuse

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

145. 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, prejudice-based and discriminatory bullying);
  - abuse in intimate personal relationships between peers;
  - 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 and Sexual violence and sexual harassment between children in schools and colleges sets out how schools and colleges should respond to reports of sexual violence and sexual harassment;
  - Consensual and non-consensual sharing of nudes and semi-nude images and/or videos[36] (also known as sexting or youth produced sexual imagery): the policy should include the school or college's approach to it. The Department provides Searching Screening and Confiscation Advice for schools. The UKCIS Education Group has published Sharing nudes and semi-nudes: advice for education settings working with children and young people which outlines how to respond to an incident of nudes and semi-nudes being shared;
  - causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party
  - upskirting (which is a criminal offence[37]), which typically involves taking a picture under a person's clothing without their permission, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress, or alarm; and
  - initiation/hazing type violence and rituals.

Advice

As previously referred to, 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, sexual violence and harassment, the sharing of nudes and upskirting. 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.

In relation to the consensual/non-consensual sharing of nudes, both the UKSIC and UKCIS resources highlighted under 'Safeguarding Issues' on pages 5-8 above are excellent supporting resources to support Schools and Colleges with this aspect. Where escalation of incidents to the Police may potentially be required, this should follow defined safeguarding procedures (i.e. escalation via the Designated Safeguarding Lead). DSLs should therefore ensure they are expressly familiar with national guidance and recommended good practice. The UKCIS guidance is particularly useful in this regard and provides comprehensive guidance with best practice case studies for schools.

Resources:

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

UKCIS > Sharing nudes and semi-nudes (December 2020)
Comprehensive advice for education settings outlining how to manage and respond to incidents of nudes and semi-nudes being shared
https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people

DfE > Sexual violence and sexual harassment between children in schools and colleges (updated guidance from Sept 2021)
Comprehensive DfE advice for education settings explaining what sexual violence and sexual harassment is, how to minimise the risk of it occurring and what to do when it does occur or is alleged to have occurred
https://www.gov.uk/government/publications/sexual-violence-and-sexual-harassment-between-children-in-schools-and-colleges

---

Children with special educational needs and disabilities or physical health issues

185. Children with special educational needs or disabilities (SEND) or certain health conditions 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 condition without further exploration;
- these children being more prone to peer group isolation or bullying (including prejudice-based bullying) than other children;
- the potential for children with SEND or certain medical conditions being disproportionally impacted by behaviours such as bullying, without outwardly showing any signs; and
- communication barriers and difficulties in managing or reporting these challenges.

Advice

Research informs us that children with special educational needs or disabilities can be particularly vulnerable to the risks posed via 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 Connecting Safely Online 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.

Relatedly, a particularly useful suite of resources is available through the Inclusive Digital Safety hub, which includes a very useful Index of Online Harms to highlight indicators and behaviours that may be of concern along with suggested interventions and escalations.

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

Internet Matters/SWGfL > Inclusive Digital Safety (IDS)
Targeted resources and guidance specifically designed for adults supporting children with SEND, those in minority groups such as the LGBTQ+ community and those who have care experience
https://www.internetmatters.org/inclusive-digital-safety

Part four: Allegations made against/Concerns raised in relation to teachers, including supply teachers, other staff, volunteers and contractors

Confidentiality and information sharing

[…]

378. The legislation prevents the "publication" of material by any person that may lead to the identification of the teacher who is the subject of the allegation. "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). In circumstances where schools need to make parents aware about an allegation, they should make parents and others aware that there are restrictions on publishing information.

Low Level concerns

[…]

409. The term 'low-level' concern does not mean that it is insignificant, it means that the behaviour towards a child does not meet the threshold set out at paragraph 338. A low-level concern is any concern – no matter how small, and even if no more than causing a sense of unease or a 'nagging doubt' - that an adult working in or on behalf of the school or college may have acted in a way that:

- is inconsistent with the staff code of conduct, including inappropriate conduct outside of work, and
- does not meet the allegations threshold or is otherwise not considered serious enough to consider a referral to the LADO.

410. Examples of such behaviour could include, but are not limited to:

- being over friendly with children;
- having favourites;
- taking photographs of children on their mobile phone;
- engaging with a child on a one-to-one basis in a secluded area or behind a closed door; or,
- using inappropriate sexualised, intimidating or offensive language.

411. Such behaviour can exist on a wide spectrum, from the inadvertent or thoughtless, or behaviour that may look to be inappropriate, but might not be in specific circumstances, through to that which is ultimately intended to enable abuse.

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).

Advice:

As is highlighted under Low Level concerns, ensuring all staff clearly understand the school's code of conduct and what is considered appropriate/inappropriate behaviour is very important. Whilst schools will have local policies relating to expectations and behaviours surrounding personal devices and social media

use, it is strongly recommended that only school-provided devices and authorised social media accounts should be used for school-related activity (e.g. the taking/posting of photographs on school trips).

Part five: Child on child sexual violence and sexual harassment

428. This part of the statutory guidance is about how schools and colleges should **respond to all reports and concerns** of child on child sexual violence and sexual harassment, including those that have happened outside of the school or college premises, and or online (what to look out for, and indicators of abuse are set out in Part one of this guidance).

429. Sexual violence and sexual harassment can occur between two children of **any age and sex**, from primary through to secondary stage and into colleges. It can 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 face to face (both physically and verbally) and are never acceptable. As set out in Part one of this guidance, all staff working with children are advised to maintain an attitude of **'it could happen here'**.

Advice

The section on child on child sexual violence and harassment has been significantly revised for 2021 and it is clear that the online environment sees repeated reference. The section highlights that sexual violence and harassment exist on a continuum and may overlap - as referred to previously, this underlines the importance of ensuring the DSL is fully informed to ensure that they are able recognise and respond appropriately to any related safeguarding concerns.

Responding to the report

[…]

443. It is essential that **all** victims are reassured that they are being taken seriously, regardless of how long it has taken them to come forward and that they will be supported and kept safe. Abuse that occurs online or outside of the school or college should not be downplayed and should be treated equally seriously. A victim should never be given the impression that they are creating a problem by reporting sexual violence or sexual harassment. Nor should a victim ever be made to feel ashamed for making a report or their experience minimised.

444. As per Part one of this guidance, all staff should be trained to manage a report. Local policies (and training) will dictate exactly how reports should be managed. However, effective safeguarding practice includes:

- if possible, managing reports with two members of staff present, (preferably one of them being the designated safeguarding lead or a deputy). However, this might not always be possible;
- where the report includes an online element, being aware of searching screening and confiscation advice (for schools) and UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people. **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. In some cases, it may be more appropriate to confiscate any devices to preserve any evidence and hand them to the police for inspection;

[…]

Action following a report of sexual violence and/or sexual harassment

What to consider

448. As set out above, sexual violence and sexual abuse can happen anywhere, and all staff working with children are advised to maintain an attitude of '**it could happen here.** Schools and colleges should be aware of, and respond appropriately to **all** reports and concerns about sexual violence and/or sexual harassment both online and offline, including those that have happened outside of the school/college. The designated safeguarding lead (or deputy) is likely to have a complete safeguarding picture and be the most appropriate person to advise on the school's or college's initial response. […]

Advice

As is highlighted, it is essential that any abuse that happens online or outside of the school environment should be treated as seriously as if it were to happen within school and this section again references the DfE searching, screening and confiscation of devices guidance.

Experience shows that even with the best of intentions, appropriately managing instances of sharing nudes can be problematic. The highly-recommended UKCIS sharing nudes guidance contains some extremely useful advice and guidance on managing instances including the process for handling incidents, responding to disclosures, setting up review meetings and carrying out an assessment of the risks.

Resources:

Department for Education

DfE > Sexual violence and sexual harassment between children in schools and colleges (updated guidance from Sept 2021)
Comprehensive DfE advice for education settings explaining what sexual violence and sexual harassment is, how to minimise the risk of it occurring and what to do when it does occur or is alleged to have occurred
https://www.gov.uk/government/publications/sexual-violence-and-sexual-harassment-between-children-in-schools-and-colleges

The end of the criminal process

[…]

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

Ongoing response

Safeguarding and supporting the victim

456. The following principles are based on effective safeguarding practice and should help shape any decisions regarding safeguarding and supporting the victim.

[…]

- Internet Watch Foundation works internationally to remove child sexual abuse online images and videos and offers a place for the public to report them anonymously.
- Childline / IWF: Remove a nude image shared online Report Remove is a free tool that allows children to report nude or sexual images and videos of themselves that they think might have been shared online, to see if they can be removed from the internet.

Advice

Page 111 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 context of the school/college's Acceptable Behaviour Agreement which should outline expected standards of behaviour both within and outside of the school environment.

KCSIE para 456 includes a variety of important principles to consider when safeguarding and supporting the victim as well as potential areas of support and includes reference to the Internet Watch Foundation (IWF) who may be able to support removing illegal images.

Additionally, the guidance also refers to the newly available Childline/IWF Report Remove facility. Report Remove is an extremely useful resource that allows those under 18 to report nude or sexual images of themselves to see if they can be removed from the internet. As well as being a useful supporting tool when responding to concerns, it is recommended that (where appropriate) schools and colleges consider raising awareness of the Report Remove facility as part of the wider approach to online safety.

Resources:

IWF > Removing illegal content
Anonymous reporting portal provided by the Internet Watch Foundation to report child abuse images and content.
https://www.iwf.org.uk/

Childline/IWF > Report Remove
Reporting facility allowing those under 18 to make a report of nude images or videos that have been shared online.
https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/remove-nude-image-shared-online/

Safeguarding and supporting the alleged perpetrator(s) and children and young people who have displayed harmful sexual behaviour

464. Advice about safeguarding and supporting the alleged perpetrators is also set out in departmental advice: Sexual violence and sexual harassment between children at schools and colleges. The following principles are based on effective safeguarding practice and should help shape any decisions regarding safeguarding and supporting the alleged perpetrator(s):
[…]

- The Lucy Faithfull Foundation has developed a HSB toolkit, which amongst other things, provides support, advice and information on how to prevent it, links to organisations and helplines, resources about HSB by children, internet safety, sexual development and preventing child sexual abuse.

Advice

As part of the response to supporting alleged perpetrators displaying Harmful Sexual Behaviour (HSB), the guidance makes reference to the Lucy Faithfull Foundation and the HSB Toolkit. The toolkit provides a range of useful tips and suggestions for responding to concerns including sex & relationships, pornography, social worlds and online behaviours.

Resources:

Lucy Faithfull Foundation > HSB Toolkit
Toolkit resource to support parents, carers, family members and professionals when addressing harmful sexual behaviours.
https://www.stopitnow.org.uk/wp-content/uploads/2020/10/Stop_It_Now_harmful_sexual_behaviour_prevention_toolkit_Oct_2020.pdf

---

Annex B: Further information

County lines

County lines is a term used to describe gangs and organised criminal networks involved in exporting illegal drugs using dedicated mobile phone lines or other form of "deal line". This activity can happen locally as well as across the UK - no specified distance of travel is required. Children and vulnerable adults are exploited to move, store and sell drugs and money. Offenders will often use coercion, intimidation, violence (including sexual violence) and weapons to ensure compliance of victims.

[…]
Children are also increasingly being targeted and recruited online using social media. Children can easily become trapped by this type of exploitation […]

Advice

Annex B refers to a variety of safeguarding issues and specific forms of abuse which include a number of references to the online environment. The section on County Lines refers to the exploitation of children and young people as part of the organised criminal networks and highlights the targeting and subsequent recruitment via online channels such as social media.

Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen off-line but are enabled at scale and at speed on-line) or 'cyber dependent' (crimes that can be committed only by using a computer). Cyber-dependent crimes include;

- unauthorised access to computers (illegal 'hacking'), for example accessing a school's computer network to look for test paper answers or change grades awarded;
- denial of Service (Dos or DDoS) attacks or 'booting'. These are attempts to make a computer, network or website unavailable by overwhelming it with internet traffic from multiple sources; and,
- making, supplying or obtaining malware (malicious software) such as viruses, spyware, ransomware, botnets and Remote Access Trojans with the intent to commit further offence, including those above.

Children with particular skill and interest in computing and technology may inadvertently or deliberately stray into cyber-dependent crime.

If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the Cyber Choices programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Note that **Cyber Choices** does not currently cover 'cyber-enabled' crime such as fraud, purchasing of illegal drugs on-line and child sexual abuse and exploitation, nor other areas of concern such as on-line bullying or general on-line safety.

Additional advice can be found at: Cyber Choices, 'NPCC - When to call the Police' and National Cyber Security Centre - NCSC.GOV.UK

Advice

As referred to on pages 24-25 of this guidance, Cybercrime is a new addition for KCSIE 2021. It is broken down into two main aspects of 'cyber-enabled' (where technology is used to enhance another type of crime (e.g. fraud)) and 'cyber dependent' (where crimes are dependent on the use of technology (e.g. illegal hacking)).

The section specifically references potential concerns around those C&YP with a particular affinity or interest in technology being inadvertently drawn into cybercrime along with available support routes. The Cyber Choices programme is particularly useful and provides resources to support Under 12s, 12–17s and over-18s, as well as resources to help support parents and carers.

Resources:

NCA > Cyber Choices

A National programme to help people make informed choices and to use their cyber skills in a legal way.

https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices

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.

- **Extremism**[130] is the vocal or active opposition to our fundamental values including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. This also includes calling for the death of members of the armed forces.
- **Radicalisation**[131] refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.
- **Terrorism**[132] is an action that endangers or causes serious violence to a person/people; causes serious damage to property; or seriously interferes or disrupts an electronic system. The use or threat must be designed to influence the government or to intimidate the public and is made for the purpose of advancing apolitical, religious or ideological cause.

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[133] to the need to prevent people from being drawn into terrorism".[134] 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 in schools 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). Designated safeguarding leads and other senior leaders in colleges should familiar themselves with the Prevent duty guidance: for further education institutions in England and Wales. The guidance is set out in terms of four general themes: risk assessment, working in partnership, staff training, and IT policies.
[…]

Advice

This section of Annex B 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 (updated April 2021). 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 remains 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

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/

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

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 on page 22 above.

A number of filtering and monitoring system providers have engaged 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 23 of this guidance.

Peer on peer/ child on child abuse

Children can abuse other children (often referred to as peer on peer abuse) and it can take many forms. It can happen both inside and outside of school/college and online. It is important that all staff recognise the indicators and signs of peer on peer abuse and know how to identify it and respond to reports. This can include (but is not limited to): bullying (including cyberbullying, prejudice-based and discriminatory bullying); abuse within intimate partner relationships; physical abuse such as hitting, kicking, shaking, biting, hair pulling, or otherwise causing physical harm; sexual violence and sexual harassment; consensual and non-consensual sharing of nudes and semi-nudes images and/or videos; causing someone to engage in sexual activity without consent, such as forcing someone to strip, touch themselves sexually, or to engage in sexual activity with a third party; upskirting and initiation/hazing type violence and rituals. Addressing inappropriate behaviour (even if it appears to be relatively innocuous) can be an important intervention that helps prevent problematic, abusive and/or violent behaviour in the future.

Advice

As previously referred to, abuse can be perpetrated by children as 'peer-on-peer' abuse and all staff should be able to recognise the signs and indicators. The section clearly references that such abuse can occur both inside and outside of the school/college as well as occurring online and makes specific reference to the consensual/non-consensual sharing of nudes/semi-nudes. All staff should know and understand how to respond to concerns and be clear about the school's safeguarding protocols in managing such instances.

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 from primary to secondary stage and into colleges. It can also occur online. It can also occur through a group of children sexually assaulting or sexually harassing a single child or group of children.

Children who are victims of sexual violence and sexual harassment will likely find the experience stressful and distressing. This will, in all likelihood, adversely affect their educational attainment and will be exacerbated if the alleged perpetrator(s) attends the same school or college. Sexual violence and sexual harassment exist on a continuum and may overlap, they can occur online and face to face (both physically and verbally) and are never acceptable.

[…]

Staff should be aware that some groups are potentially more at risk. Evidence shows girls, children with special educational needs and disabilities (SEND) and LGBT children are at greater risk.

Staff should be aware of the importance of:

- challenging inappropriate behaviours;
- making clear that sexual violence and sexual harassment is not acceptable, will never be tolerated and is not an inevitable part of growing up;
- not tolerating or dismissing sexual violence or sexual harassment as "banter", "part of growing up", "just having a laugh" or "boys being boys"; and
- challenging physical behaviours (potentially criminal in nature), such as grabbing bottoms, breasts and genitalia, pulling down trousers, flicking bras and lifting up skirts. Dismissing or tolerating such behaviours risks normalising them.

[…]

Sexual harassment

When referring to sexual harassment we mean 'unwanted conduct of a sexual nature' that can occur online and offline and both inside and outside of school/college. When we reference sexual harassment, we do so in the context of child on child sexual harassment. Sexual harassment is likely to: violate a child's dignity, and/or make them feel intimidated, degraded or humiliated and/or create a hostile, offensive or sexualised environment.

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

[…]

- online sexual harassment. This may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence.[139] It may include:
    - consensual and non-consensual sharing of nudes and semi-nudes images and/or videos.[140] As set out in UKCIS Sharing nudes and semi-nudes: advice for education settings working with children and young people (which provides detailed advice for schools and colleges) taking and sharing nude photographs of U18s is a criminal offence;
    - sharing of unwanted explicit content;
    - upskirting (is a criminal offence[141]);
    - sexualised online bullying;
    - unwanted sexual comments and messages, including, on social media;
    - sexual exploitation; coercion and threats.

Advice

As is apparent from the above extract, sexual violence and sexual harassment between children includes a significant number of online elements. This section highlights 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 consensual and 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 end of the sexual violence and harassment section on page 142 of KCSIE 2021 includes a very useful Toolkit section that provides a variety of references and lesson resources that can help to support schools and colleges.

Upskirting[142]

The Voyeurism (Offences) Act 2019, 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 sex, can be a victim.

Advice

The section on Upskirting, originally introduced in 2019 makes specific reference to The Voyeurism (Offences) Act 2019. *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:

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

Advice

Annex B (Further information) includes a wide variety of important additional information about specific forms of abuse and safeguarding issues. Of particular note, pages 142-144 include a number of additional advice and support references which are mapped against each of the related sections of Annex B. In relation to the online environment, these include reference to Preventing Bullying (including cyberbullying), Health & Wellbeing (Rise Above) and Radicalisation.

Annex C: Role of the designated safeguarding lead

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.[143] 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. […]

Working with others

The designated safeguarding lead is expected to:

[…]

- act as a source of support, advice and expertise for all staff;
- act as a point of contact with the safeguarding partners;
- liaise with staff (especially teachers, pastoral support staff, school nurses, IT Technicians, senior mental health leads and special educational needs co-ordinators (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 so that children's needs are considered holistically;

[…]

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, including the safeguarding partners. 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.

Raising 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; and

Advice

Maintaining links with the safeguarding partnership arrangements is highlighted as a role for the DSL. Replacing the former LSCB arrangements, the Children's Safeguarding Assurance Partnership also has a 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 Web pages (new website due Autumn 2021)
Dedicated online safety section to support colleagues in schools, colleges and the wider children's workforce
https://www.safeguardingpartnership.org.uk/online

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
https://www.safeguardingpartnership.org.uk/learn

Training, knowledge and skills

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, how to identify, understand and respond to specific needs that can increase the vulnerability of children, as well as specific harms that can put children at risk, and the processes, procedures and responsibilities of other agencies, particularly children's social care, so they:

[…]

- are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college;
- can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support children with SEND 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 CSAP 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
https://www.safeguardingpartnership.org.uk/online/#OS_NewsEvents

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 previous 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 remains relevant and provides invaluable information which can be used to help inform staff awareness sessions as well as providing a stimulus to developing similar local activities in school.

Resources:

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
https://www.safeguardingpartnership.org.uk/online/resources/#OtherResources

---

Annex D – Online Safety

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
[…]
Remote education, virtual lessons and live streaming
[…]
Support for children
[…]
Parental support
[…]

Advice

As referred to on page 19 above, previous versions of KCSIE contained Online Safety as a separate Annex (Annex C). For KCSIE 2021, this has now been included as a core aspect in the main body of the statutory

guidance. However, as can be seen from Annex D above, a dedicated annex remains which is now used to provide over 30 useful signposts to related information and support, grouped around four areas.

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 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 15 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 maintained 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. In addition, CSAP maintains an active social media presence via Twitter which provides a variety of safeguarding-related updates, including regular updates on online safety.

Resources:

CSAP > Online Safeguarding Web pages
Dedicated online safety section to support colleagues in schools, colleges and the wider children's workforce
https://www.safeguardingpartnership.org.uk/online

CSAP > Twitter
Lancashire Safeguarding Twitter account providing the latest Safeguarding related news and updates including Online Safety
https://twitter.com/csap_lsab

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. On a broader level, the online environment is an integral part of modern life and as such, in order to effectively address on a child-centric level, we should consider a contextual approach to safeguarding in relation to those factors and influences that surround our children and young people.

All of the above highlighted resources are available via the Online Safeguarding section of the CSAP website and whilst this guidance does not seek to be exhaustive, it is intended to provide colleagues with comprehensive guidance and support 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
Children's Safeguarding Assurance Partnership
September 2021

e-mail: graham.lowe2@lancashire.gov.uk
web: https://www.safeguardingpartnership.org.uk
twitter: @CSAP_LSAB

Children's Safeguarding Assurance Partnership
Blackburn with Darwen - Blackpool - Lancashire

Further advice and information about Online Safety is available from the CSAP Online Safeguarding homepage at:
https://www.safeguardingpartnership.org.uk/online

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 2021. 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.