This guidance has been produced in response to common queries received from school-based colleagues around policy guidance, tools and recommended resources to support schools in addressing the online aspects of radicalisation and extremism. The guidance is specifically aimed to underpin its inclusion within existing good practice for online safety and also, to embed within the broader school safeguarding provision in line with the Strategic Objectives of the Pan-Lancashire LSCB eSafeguarding Strategy.

**Context:** This guidance, whilst specifically relating to the online aspects of radicalisation/extremism, is designed to be set within the context of developing, and being complementary to, the overarching school Safeguarding provision. Included at the end of this guidance are links to both the resources referred to and additional useful resources. The Strategic Objectives outlined opposite provide a useful basis to structure addressing the online aspects though it is important to recognise that the objectives are **not mutually exclusive** and should therefore ultimately be viewed holistically when reviewing provision. However, a number of the resources referred to are structured with similar aspects and therefore provide a complementary approach across the various areas. This guidance provides an outline against these Strategic Objectives with potential Considerations ( _) and suggested Recommendations ( _) within each section.

With varying approaches, the online environment is used to engage and radicalise young people. The use of often slick and professionally-produced propaganda materials, combined with prolific use of Social Media platforms mean that extremist organisations are able to target young people on a scale previously unseen and can exaggerate their scale or influence at relatively low cost. The messages can follow the style of product marketing campaigns including brand recognition and emotional engagement, seeking to exploit vulnerabilities, disillusionment or confused perceptions. Videos and photographs typically feature heavily, and combined with the perceived real-time nature of Social Media, serve to engender a direct link to events.

**Grooming:** Often similar to those methods used in online grooming in respect of Child Sexual Exploitation, to develop further engagement, group individuals may encourage the young person to move from the initial ‘broadcast’ medium (e.g. public forum, one-2-many, social network) to a ‘direct’ medium (e.g. one-2-one, direct messaging, secure platform). Furthermore, the young person may perceive themselves to be willingly engaged rather than recognising the underlying manipulation or coercion involved. The psychological aspects that surround an individual’s susceptibility to be drawn into supporting terrorism are varied, including those factors outlined opposite. In

---

To view the full document, visit: [www.preventforschools.org](http://www.preventforschools.org)

---

HM Govt, Channel Duty Guidance 2015

---

Lancashire Safeguarding Children Board

---

© Lancashire Safeguarding Children Board 2016
addition, the individual’s social environment may amplify such vulnerabilities by legitimising and normalising such behaviour. Extremist organisations often employ technology, particularly Social Media, as an ideal medium to engage with a broad audience. The use of technology is often highly articulate, significantly engaging and professionally produced, allowing groups to maximise engagement and seek to legitimise their extremist ideology. As young people are significantly invested in Social Media (though have not necessarily developed the broader life experience and critical thinking skills), they present a particular concern especially where they have particular vulnerabilities which extremist organisations seek to exploit.

Guidance is clear that there is ‘...no single route to terrorism nor is there a simple profile of those who become involved.’ In looking at broad indicators of engagement, we can see that the majority are also transferable to an online context which, without detailed knowledge, can be challenging to differentiate from typical adolescent behaviour (e.g. spending large amounts of time online, protective about online behaviour, less ‘real world’ engagement, identifying with other online users/groups etc). With this in mind, it is therefore important that we address concerns within the context of existing Safeguarding practices and procedures.

Escalation and Support: As identified, reporting concerns relating to potential online aspects of radicalisation and extremism should follow established Safeguarding procedures within school which may determine further escalation to support routes such as Channel. Where appropriate, the DfE provide a dedicated telephone and e-mail helpline for school staff and governors to report extremism concerns directly (details are available in the DfE Departmental Advice resource). Reporting online terrorist material can be done using the HM Government online reporting button opposite which provides an anonymous, simple to-use interface.

Professionals who would like support with broader online safety concerns can contact the UK Safer Internet Centre Professionals Online Safety Helpline (POSH) who can advise on options available. This may include advice around online bullying, sexting, gaming or broader social media issues.

The ACPO site ‘True Vision’ can be used to report hate crimes or hate incidents and includes useful guidance about what hate crimes are and ways they can be reported. [www.report-it.org.uk](http://www.report-it.org.uk)

**Approach:** Experience illustrates that the most effective approaches are where online risks are addressed with a Safeguarding perspective rather than from an ICT approach. Whilst the online world may seem complex or be unfamiliar territory for many, it is useful to remember that online risks fundamentally remain SAFEGUARDING issues.

This resource has been made possible through the support of Lancashire localities group colleagues across the Blackpool; Chorley; Fylde; Hyndburn; Lancashire; Lancaster; Pendle; Preston; Rossendale; South Ribble; West Lancashire and Wyre regions. The nature of the online environment and its use is constantly evolving and therefore whilst not intended to be exhaustive, it is hoped that you will find this a useful and informative resource to support further progression in our shared aims of safeguarding our children and young people online.
In March 2015, the Government revised the Prevent Duty, outlining the statutory duties placed on a variety of specified authorities (including Schools). Further to this, the DfE subsequently issued non-statutory departmental advice for schools and childcare providers outlining a number of areas for focus which include Staff Training, IT Policies and building Children’s Resilience.

**Policies (General):** Policies outlining the school’s duties and approach to Safeguarding should be clear and communicated to all Stakeholders (SLT, Governors, Staff, Pupils/Students, Parents/Carers). These should explicitly reference online risks including online radicalisation/extremism. It is also important to ensure that extremism is considered in its broader sense of ideologies that encourage violence to influence change (e.g. including, but not limited to, Far Right extremism, Islamist extremism, Environmental extremism, Northern Ireland-related extremism, Animal Rights extremism etc).

*(Note: The Prevent duty referred to above does NOT require a separate ‘Prevent Policy’).*

**Online Safety Policies:** School Online Safety Policies need to be developed to reflect individual school requirements and expectations. The SWGfL Template policy provides an excellent, comprehensive and considered basis to addressing online safety and is a highly recommended (freely available) resource. The template also includes a large variety of appendices covering various topics including Acceptable Use Agreements, Incident flowcharts, Technical Security, BYOD and Personal Data policy templates. The resource also includes guidance notes to aid colleagues in completion. As protecting Children and Young People from radicalisation and extremism is fundamentally a Safeguarding issue, it is essential that related policies and procedures are consistent and provide a robust approach.

**Expectations:** Online Risks for Children and Young People (C&YP) do not begin or end at the school gates nor are they limited by geographic borders or boundaries. Consequently, our approach to safeguarding C&YP must be equally applicable in order to support them and build resilience to online threats. The stakeholders mentioned above must be clear about the school’s expectations both inside and outside of school and this should be reflected in related policies (e.g. behaviour management policies, staff codes of conduct, home-school agreements, anti-bullying policies etc).

- Consider…involving Pupil/Student bodies (e.g. school council) in developing policies and procedures. Ensure this is referenced in the resulting documents.

- Consider…an adapted or summary version of policies and procedures suitable for pupils/students

**Responsibility:** Whilst the Online Safety agenda may traditionally be perceived in school as a role for the ICT Coordinator, effective practice typically shows this is most effective when it is a collaborative approach with a Safeguarding rather than ICT lead.
Acceptable Use Policies/Agreements: Historically, whilst these have typically been focussed around the acceptable use of school-owned equipment (i.e. the Do’s and Don’ts), the increasing use of personal technology in the school environment needs careful consideration. In this respect, revising the agreements to acceptable ‘behaviour’ rather than acceptable ‘use’ can provide a useful and broader focus for what online activity is allowed within the school environment. With a focus on behaviour when using technology, it is useful to align and complement what is acceptable with the school’s stated values and ethos and also, those areas outlined in the school’s Behaviour Management Policy (and vice-versa) thereby creating robust, complementary arrangements.

✓ Safer Management Recommendations:

- Develop the school’s Online Safety Policy using the SWGfL School Online Safety Template Policy, adapting to local requirements. Ensure related policies are complementary and provide a robust, consistent approach (see also Safer Standards Recommendations re: 360° Safe Self Review Tool).

- Review and align existing Acceptable Use Policies/Agreements in line with the above. Ensure the renewed policy/agreement takes account of extreme content and explicitly highlights the school’s expectations in this respect. Highlight that the sharing of such content by students (including personally-owned devices, smartphone, social media, messaging apps etc) is unacceptable behaviour.

- ‘eSafety’ is largely outdated terminology. When reviewing existing policies, use ‘Online Safety’ as a more appropriate and meaningful term.

- Ensure Staff Online Safety INSET and Parental Awareness Sessions include explicit reference to the potential risks around online radicalisation and extremism as part of the broader online safety messages (see also Safer Learning).
Safer Access

The aforementioned departmental advice from the DfE outlines expectations across a number of areas including IT policies and highlights: [DfE 2015: “The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place.”].

In promoting Safer Access, schools should address both Technical aspects (e.g. content filters, network monitoring tools) and non-Technical aspects (e.g. supervision, lesson planning, curriculum delivery). These aspects can also present a useful learning opportunity under the Safer Learning priority to discuss “why there is a need to filter online content” and “why we should develop Digital Literacy”.

Content Filtering Systems: In considering content filtering tools, it is useful to understand their function and more importantly, their purpose. A content filter typically provides filtered internet access through a series of pre-determined algorithms and are based around the categorisation of websites which are subsequently applied according to block or allow policies. As a combination of software and hardware tools, these are increasingly sophisticated systems. However, it is essential to understand that their purpose is to mitigate the potential for access to inappropriate or illegal content. As such, a content filter is NOT a solution and in order to be effective, should complement robust teaching and learning practices to support children’s safe use of the Internet.

In addition, the ability to locally manage filtering policies provides increased flexibility appropriate to school requirements. Whilst this must be considered in the context of maintaining appropriate safeguards, this can support transition from ‘locked-down’ to ‘managed’ systems in school.

Differentiation: A one-size-fits-all approach to filtering is not appropriate and schools should be careful that overblocking does not lead to an adverse impact on teaching and learning. Pupils and Students will understandably require increasingly less restrictive policies as they progress.

Consider...differentiated levels of filtering policy for pupils/students on curriculum networks. Additionally, access to sites typically blocked to pupils on the curriculum network (e.g. YouTube), may provide useful learning resources and therefore, subject to appropriate safeguards, could be made accessible to staff through the Staff filtering policy.

Consider...whether the school’s chosen provider offers the facility to locally manage policies to block / allow specific websites at the school level (where appropriate).

Network Monitoring Systems: Network monitoring systems are increasingly sophisticated and can provide a useful addition to supporting Safer Access priorities. This is both in monitoring actual network activity as it occurs and also in encouraging positive behaviour when using school systems through the user’s knowledge that activity is being monitored. Systems can be locally managed in school or through a third-party provider, though both options require robust policies and procedures to be in place prior to implementation (including defined escalation and management protocols) with a safeguarding-led responsibility.

Note: At the time of development (March 2016), the results of the DfE consultation on proposed changes to ‘Keeping Children Safe in Education’ (KCSIE) are yet to be announced. Dependent on outcomes, the proposed changes potentially see a number of implications for school-based colleagues in relation to content filtering and monitoring requirements. This guidance will therefore be updated to reflect the consultation outcomes where applicable as they become available.
What is ‘appropriate’? Under the revised Prevent Duty 2015, Schools (and registered childcare providers) in England and Wales are required to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering. and this aspect is further emphasised within the draft DfE KCSIE consultation highlighted previously. Colleagues at the UK Safer Internet Centre (UKSIC) have produced two highly recommended resources to support schools with assessing filtering and monitoring provision, highlighting related aspects and recommendations.

Personal Devices: The use of personally-owned devices in school is typically widespread and where covered in existing policies or procedures, may not highlight the potential risks posed from extremist content. As these devices do not typically utilise the school’s technical infrastructure and therefore its inherent safeguards, behaviour expectations of students need to be considered as per the Acceptable Behaviour consideration previously highlighted.

Consider...whether existing policies and procedures address expectations for the use of personal devices within the school for staff, students and visitors in respect of extremism.

Safer Access Recommendations:

In order to both ensure and evidence that suitable filtering is in place, schools should obtain confirmation from their chosen Internet Service Provider or content filtering supplier that the filtering product supplied meets the requirements of the revised Home Office Prevent Duty 2015. In progressing provision, it is recommended schools investigate filtering providers who implement the ‘police assessed list of unlawful terrorist content, produced on behalf of the Home Office’.

Utilise the Safer Internet Centre Appropriate Filtering and Monitoring resources in assessing the school’s provision as part of developing a robust risk assessment.

Schools providing facilities to external users should review internet access in their policies and procedures to ensure they cover radicalisation/extremism. Terms and conditions of use should clearly identify both the provision (e.g. filtered access, monitoring systems (where applicable)) and the school’s expectations of users (e.g. users will not attempt to circumvent the school’s safeguarding and security measures).

Review existing policies and procedures where appropriate, to address expectations for the use of personal devices within the school for staff, students and visitors.
Core aspects of protecting and supporting our C&YP lies in raising awareness of the potential online threats and building C&YP’s resilience. Schools already do this for a variety of other online safety areas such as Online Child Sexual Exploitation, Bullying and Sexting. When looking at the factors and indicators involved, it is apparent that radicalisation is a grooming process which schools will already be familiar with. Equally, when faced with a variety of online content across the extremist spectrum, Digital Literacy education and developing Critical Thinking skills amongst learners are both key aspects. Schools already address these aspects in a variety of ways and therefore provide an existing basis from which to adapt and address the radicalisation/extremism agenda.

**Learning Opportunities**: Whilst the online aspects of radicalisation and extremism should be included when addressing the broader online safety risks, the most robust approaches are typically cross-curricular rather than limited within delivery of the Computing curriculum (e.g. History - the role of propaganda in conflicts, PSHE – developing healthy relationships).

[DfE 2015: More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school’s ICT curriculum and can also be embedded in PSHE and SRE.]

In the context of online radicalisation and extremism, critical thinking and digital literacy are especially relevant to support and develop young people’s resilience to online influences. Building and equipping pupils with the skills to critically assess online content, building resilience and making informed decisions (e.g. is everything on the Internet true?, how can I check factual accuracy?) are fundamental lifelong skills that extend and impact far beyond the school environment.

Consider...utilising resources such as The Guardian ‘Points of View’ clip to introduce or complement ‘Critical Thinking’ activities.

The Guardian Advert ‘Points of View’ (1986): 30-second clip by The Guardian newspaper illustrating different perspectives v the whole picture (see: www.youtube.com/watch?v=_SscRkLLzU)

**Addressing Online Extremism through Digital Literacy**: A highly recommended classroom resource developed by colleagues at Childnet International to address Critical Thinking skills in Young People and what they see online, was released in May 2016. Further details on the resource are available from the P4S site (www.preventforschools.org) ‘Other Recommended Resources’ section.

In addition, the SWGfL Digital Literacy and Citizenship resources available at www.digital-literacy.org.uk provide some excellent, freely available resources from Foundation Stage through to Year 10 to support schools across a variety of aspects.

Annual events such as Safer Internet Day in February provide a useful and dedicated opportunity to timetable and discuss online risks including online radicalisation and extremism.
Consider...planning a ‘week of action’ to coincide with Safer Internet Day, addressing a
different aspect of online safety on each day (e.g. Grooming, Bullying, Radicalisation,
Sexting, Gaming, Social Media) culminating in a review of activities and learning outcomes
on the final day of the week through assembly activities.

Consider...Parent/Carer Engagement - Safer Internet Day typically attracts significant national
media attention and offers the opportunity to engage with Parents/Carers with newsletter
updates, website announcements and maximise attendance at Parental Awareness Sessions.

Consider...encouraging safe practice by displaying items such as the school’s online safety rules,
‘what to do if something goes wrong’ instructions or the Childnet ‘SMART rules’ as the desktop
background picture.

[DfE 2015: As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of
extremist and terrorist groups.]

Staff Training: Whilst there is a natural focus on supporting C&YP, all
school staff must also receive regular and effective CPD opportunities. On the broader Prevent agenda, key staff
such as the Headteacher, Designated Safeguarding Lead and Chair of Governors may have already attended the
Home Office WRAP training. In addition, the wider workforce could complete online awareness packages such
as the ‘NCALT module’ or the newly available ‘Introduction to Prevent’ package opposite (see Resource List Appendix
provided below or access via the P4S website).

---

**Safer Learning Recommendations:**

- Ensure online safety delivery includes addressing online radicalisation and extremism along
  with broader risks such as grooming, online bullying, sexting and information privacy.
- Develop a broad, cross-curricular approach and maximise opportunities to develop critical
  thinking skills in related topics to support building resilience in pupils and students.
- Within the context of the school’s broader Safeguarding approach, ensure all staff receive
  appropriate and regular Online Safety CPD which explicitly includes reference to online
  radicalisation and extremism.
- Inform the school’s approach to Online Safety through input from pupils and students to
  ensure delivery is robust and addressing concerns.
- Ensure key staff attend update events such as the Pan-Lancashire annual Online Safety
  Briefings¹ hosted through the LSCB.

---

¹ 2017: Online Safety Briefing – Lancashire: Tuesday 17th January 2017 (further details to be circulated through the Lancashire Schools Portal,
Autumn 2016); Blackpool (Monday 16th January 2017); Blackburn with Darwen (Wednesday 18th January 2017)
As previously highlighted, schools may already be addressing many aspects highlighted in this guidance, though perhaps with a historically different emphasis (e.g. Online grooming in respect of Child Sexual Exploitation). In order to promote and ensure appropriate monitoring and review practices are in place surrounding online radicalisation and extremism, a review of effective and regularly audited procedures, tools and learning is important. As such, the Safer Standards priority is directly linked with each of the other priorities and particularly, with those areas outlined in the Safer Management aspect.

In extending existing online safety practice to address online radicalisation/extremism risks, those associated policies and procedures should be reviewed for currency (whilst not exhaustive, a list of potentially related policies has been included below for consideration). In many cases, this will require relatively minor amendments though it is important to retain a holistic overview to ensure consistent and complementary provision.

Given the changing nature of the online environment, Online Safety Policies should be reviewed at least annually. A useful and highly recommended (freely available) tool to self-assess provision is the 360°Safe Online Safety Self Review Tool. The tool follows a very similar structure to the LSCB Strategic Objectives and allows schools to self-assess and benchmark their provision across a variety of areas. The tool also includes reference to online radicalisation/extremism and provides useful suggested ‘next steps’ in progressing provision. When used with the SWGfL Online Safety Templates, the combined aspects provide a significantly comprehensive and extremely useful resource for schools.

Once schools have reviewed and updated related policies and procedures, these should be assessed to ensure they are robust and effective. In this respect, it is often useful to utilise a member of staff who has not been involved in their development to-date to ‘walk-through’ potential scenarios to ensure they effectively address potential issues and amend where required.

It is important to ensure that where incidents do occur, they are acted upon effectively. In line with broader Online Safety advice, a review of the Incident Log should be regularly carried out to ensure issues have been addressed and documented (both in terms of recording the incident itself and recording the subsequent actions taken). In support of Safer Standards, the log should be used to identify and inform future progression (e.g. if there are regular incidents involving inappropriate content, a review of both the filtering platform used and pupil access/behaviour may be appropriate).

Related Policies - Whilst schools will have a variety of local arrangements or combinations and are therefore not exhaustive, the suggestions below are primarily intended to serve as a prompt for consideration:

- Online Safety Policy (formerly known as the eSafety Policy) including Acceptable Use Agreements
- School Safeguarding/Child Protection Policy; Staff & Student Codes of Conduct; Behaviour Management Policy; Home-School Agreements; School Website/Social Media arrangements; Visitor Policy; Information Security Policy; School Governance arrangements; Anti-Bullying Policy; IT Support Provider Agreements; Staff Training/CPD Policy; Complaints Procedures; Curriculum Delivery;
Safer Standards Recommendations:

- Review existing Online Safety provision using the 360° Safe Self Review Tool. Use the findings to inform the development of the school’s Online Safety Policy (see also Safer Management Recommendations).

- Audit existing practice using ‘What if…’ scenarios and review against policies and procedures to ensure they are robust, amending where required. (e.g. ‘What if’...a pupil accessed extremist content whilst in school? ‘What if’...the school became aware of gruesome images being shared between students?)

- Review provision around both online and offline activity to ensure it is complementary. Addressing radicalisation/extremism as part of the school’s broader Safeguarding provision supports a consistent approach.

- In line with existing Safeguarding practices, check ALL staff understand the school’s procedures and processes involved in protecting pupils/students from online radicalisation and extremism.
Appendix 1: Resource List (all freely available) in order of appearance

HM Govt – Report Online Terrorist Material
https://www.gov.uk/report-terrorism

UKSIC Professionals Online Safety Helpline
www.saferinternet.org.uk/about/helpline

ACPO TrueVision Stop Hate Crime
www.report-it.org.uk/

DfE Prevent Duty Departmental Advice

SWGfL School Online Safety Template Policy
http://swgfl.org.uk/products-services/esafty/resources/creating-an-esafty-policy

UK Safer Internet Centre – Appropriate Filtering & Monitoring Advice
www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-and-monitoring

Digital Literacy & Citizenship Resources
www.digital-literacy.org.uk

Safer Internet Day Site
www.saferinternetday.org

HM Govt: Introduction to Prevent e-learning package
www.elearning.prevent.homeoffice.gov.uk

SWGIL 360° Safe Online Safety Self Review Tool
https://360safe.org.uk/

Childnet International – Be SMART on the Internet
www.childnet.com/resources/be-smart-on-the-internet

Lancashire Prevent for Schools (P4S) Site
www.preventforschools.org