

KCSIE 2023 Update for DSL's

Jatinder Matharu

Keeping children safe in education 2023

Statutory guidance for schools and
colleges

The 2022 version of the guidance is currently in force.
The 2023 version will come into force on 1 September
2023.

Keeping children safe in education 2023

Statutory guidance for schools and colleges

The 2022 version of the guidance is currently in force. The 2023 version will come into force on 1 September 2023.

Part 1: Safeguarding information for all staff

everyone should receive as part of their safeguarding and online safety training, staff need to understand their expectations, roles and responsibilities around filtering and monitoring systems

Part 2: The management of safeguarding

Children being absent from education for prolonged periods and/or on repeat can act a warning sign to a range of safeguarding issues. The guidance specifies it's important that your school's response to persistently absent pupils and children missing education supports identifying any abuse, and in the case of absent pupils, helps prevent the risks of them becoming a child missing education in future

the term '*children missing education*' is different from '*children absent from education*'

Part 3: Safer recruitment measures

Along with informing shortlisted candidates about online searches, your school should:

As part of ongoing vigilance, create the right culture so staff feel comfortable discussing safeguarding matters in and outside of work – the guidance has added that this includes online

Part 4: Handling allegations against staff

If your school receives an allegation relating to an incident where an individual or organisation was using your school premises for running an activity for children, your senior leaders should follow your safeguarding policies and procedures and inform the local authority designated officer (LADO), as they would with any safeguarding allegation.

Part 5: Child-on-child sexual violence and sexual harassment

The word 'sanction' has replaced the word 'discipline' to reflect the most recent behaviour guidance



Summary of changes in KCSIE 2023

Children missing education and children absent from school

Children being **absent** from education **for prolonged periods and/or on repeat occasions** can act as a vital warning sign to a range of safeguarding issues including neglect, child sexual and child criminal exploitation - particularly county lines. It is important the school or college's response to **persistently absent pupils and children missing education** supports identifying such abuse, **and in the case of absent pupils, helps prevent the risk of them becoming a child missing education in the future**. This includes when problems are first emerging but also where children are already known to 45 local authority children's social care and need a social worker (such as a child who is a child in need or who has a child protection plan, or is a looked after child), **where being absent from education** may increase known safeguarding risks within the family or in the community.

Behaviour in schools

Behaviour in Schools guidance updated September 2022 and referenced in KCSIE 2023 – **Need a Behaviour Policy and all staff should have access to this!**

Forced marriage Since February 2023, it's been a crime to carry out any conduct whose purpose is to cause a child to marry before their 18th birthday, even if violence, threats or another form of coercion are not used. This applies to non-binding, unofficial 'marriages' as well as legal marriages.



Summary of changes in KCSIE 2023

Online searches

Additional information about online searches for shortlisted candidates (added to guidance last year). May need to check with HR provider and update to the recruitment policy accordingly.

DBS certificates

Reordered about retention of documents. Copies of documents used to verify the successful candidates identity, right to work and required qualifications.

DBS **do not have** to keep copies of the DBS certificate in order to fulfil the duty of maintaining the single record.

Lettings of school premises (out of school settings OOSS)

As with any allegation, schools and colleges should follow their safeguarding policies and procedures including informing the LADO. Ensure you get their SG policy ahead of any agreement.

Radicalisation, the Prevent duty and Channel

The section on preventing radicalisation says children may be '**susceptible**' to extremist ideology and radicalisation, rather than '**vulnerable**' on preventing radicalisation. Governor update are available here: [Prevent duty training - GOV.UK \(www.gov.uk\)](https://www.gov.uk)

The Statutory Prevent duty

Guidance

Understanding and identifying radicalisation risk in your education setting

Published 24 October 2022

[Understanding and identifying radicalisation risk in your education setting - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/understanding-and-identifying-radicalisation-risk-in-your-education-setting)

Ofsted's Education & Inspection Framework

- Quality Of Education
- Leadership & management (SG & Prevent)
- Personal Development (British Values)
- Behaviour & attitudes



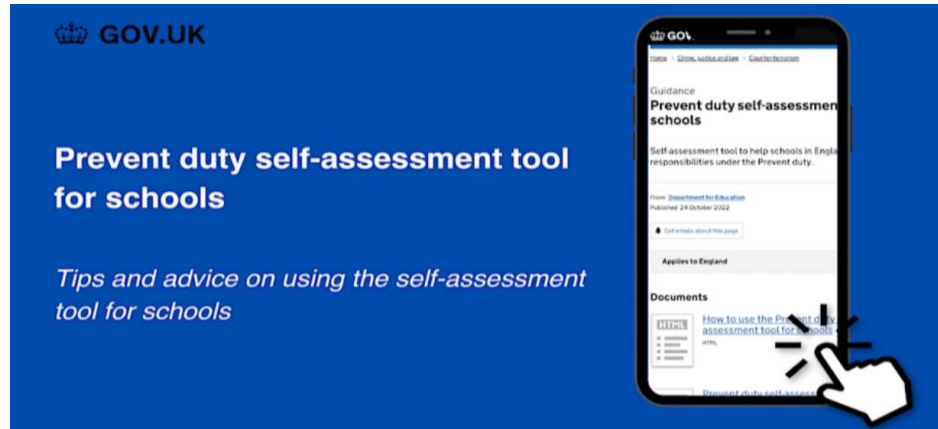
Counter Terrorism & Security Act 2015 - The Prevent Statutory Duty:

“to have due regard to the need to prevent people from being drawn into terrorism”

The Duty applies to “specified authorities” who are inspected for compliance by Ofsted (utilising their Education Inspection Framework), this of course includes schools.

- Risk Assessment
- Prevent Action Plan
- Partnership
- Staff training
- Welfare and pastoral care
- Safety online
- Speakers and events

Prevent Self-Assessment Toolkit for schools



7 Distinct areas (requirements) of judgement:

1. Leadership & Management
2. Risk Assessment
3. Working in Partnership
4. Training
5. Online Safety
6. Safeguarding School Premises
7. Building Children's Resilience to Radicalisation

[Prevent duty self-assessment tool for schools - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/prevent-duty-self-assessment-tool-for-schools)

A self-assessment tool to assist schools to review how well embedded & effective their Prevent responsibilities are in advance of Ofsted inspection.

The toolkit is NOT a replacement or alternative to a statutory Prevent risk assessment & action plan

Neglect and the cost-of-living crisis

- More families than ever are feeling the pinch of the cost of living
- More than 1 in 4 children are now living in poverty
- 54% of parents/carers have had to cut back on food spending in the last year
- 1 in 5 parents/carers are struggling to provide enough food for their children



Poverty and financial hardship are not the same as neglect – but they do increase the risk of experiencing neglect

Cost-of-living crisis: what impact is it having on our pupils?



Reporting child sexual abuse: legislation changes

- The government is currently considering changes to legislation around reporting child sexual abuse
- If these changes are approved, there will be legal implications for not reporting suspected cases of abuse
- You **must** report any signs of possible sexual abuse to your DSL **immediately**
- Always be alert for signs of child sexual abuse



If we're doing our jobs as we should, this change in legislation shouldn't change a thing about what we're doing!

Cyber security standards

- [Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges)

Cyber security standards for schools and colleges

Find out what standards your school or college should meet on cyber security, user accounts and data protection.

[Show all sections](#)

Protect all devices on every network with a properly configured boundary or software firewall

[Show](#)

Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date

[Show](#)

Accounts should only have the access they require to perform their role and should be authenticated to access data and services

[Show](#)

You should protect accounts with access to personal or sensitive operational data and functions by multi-factor

Filtering is also about cybersecurity

Cyber Security Schools Audit 2022

National Cyber
Security Centre
a part of GCHQ

LGfL

Key Findings



Cybersecurity in schools – are we teaching and learning?



Analysis and next steps from the 2022
audit of cybersecurity in UK schools

LGfL

Cyber security is linked to safeguarding because ...

We hold personal data such as registers, CP data etc..

Is your setting thinking about this?

Cyber security

You should have effective monitoring strategies that meet the safeguarding needs of your school or college.

- Schools should meet the Cyber Security Standards
- All staff should have annual Cyber Security training;
- At least one governor should also access this training

[Cyber security training for school staff - NCSC.GOV.UK](https://www.ncsc.gov.uk/cyber-security-training-for-school-staff)



The screenshot shows the National Cyber Security Centre (NCSC) website. The header is green with the NCSC logo and navigation links: ABOUT NCSC, CISP, REPORT AN INCIDENT, CONTACT US, and a search icon. Below the header is a dark green navigation bar with links: Home, Information for..., Advice & guidance, Education & skills, Products & services, and News, blogs, events... The main content area has a blue 'INFORMATION' tag and the title 'Cyber security training for school staff'. Below the title is a sub-headline: 'A cyber security training package for school staff to help improve their school's cyber resilience.' To the right of the main content are three icons: a download icon with the text 'Download / Print Article PDF', a share icon with the text 'Share', and a 'PUBLISHED' date of '21 April 2021'. Below that is a 'REVIEWED' status.



Frankie Thomas

Filtering and Monitoring standards

Filtering and monitoring standards were issued March 2023 to ensure secure and regular monitoring is in place and the filtering processes are reviewed regularly.

- “Governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place **and regularly review their effectiveness,**” **the new guidance states.**
- “They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.”

[Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK \(www.gov.uk\)](#)



New emphasis on filtering and monitoring systems.

Be aware that:

- Filtering and monitoring systems protect pupils and staff from harmful and inappropriate content online
- Harmful content may be legal or illegal, and could include:
 - Pornography
 - Promotion of self-harm and/or suicide
 - Misogyny
 - Racism
 - Fake news
 - Extremist views
- All staff should follow policies and procedures, report any problems, and monitor what's happening on screens in school

Filtering and monitoring standards

- [Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK \(www.gov.uk\)](#)

Find out what standards your school or college should meet on filtering and monitoring.

[Show all sections](#)

You should identify and assign roles and responsibilities to manage your filtering and monitoring systems

[Show](#)

You should review your filtering and monitoring provision at least annually

[Show](#)

Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning

[Show](#)

You should have effective monitoring strategies that meet the safeguarding needs of your school or college

[Show](#)

What are filtering and monitoring standards

What are they?

They provide a safe environment to learn and work by protecting pupils and staff from harmful and inappropriate content online. What's seen to be harmful will depend on each pupil.

What's my role?

All staff need to:

- Follow policies and procedures
- Report any problems
- Monitor what's happening on screens



Role of the DSL: KCSIE 2023



Department
for Education

Keeping children safe in education 2023

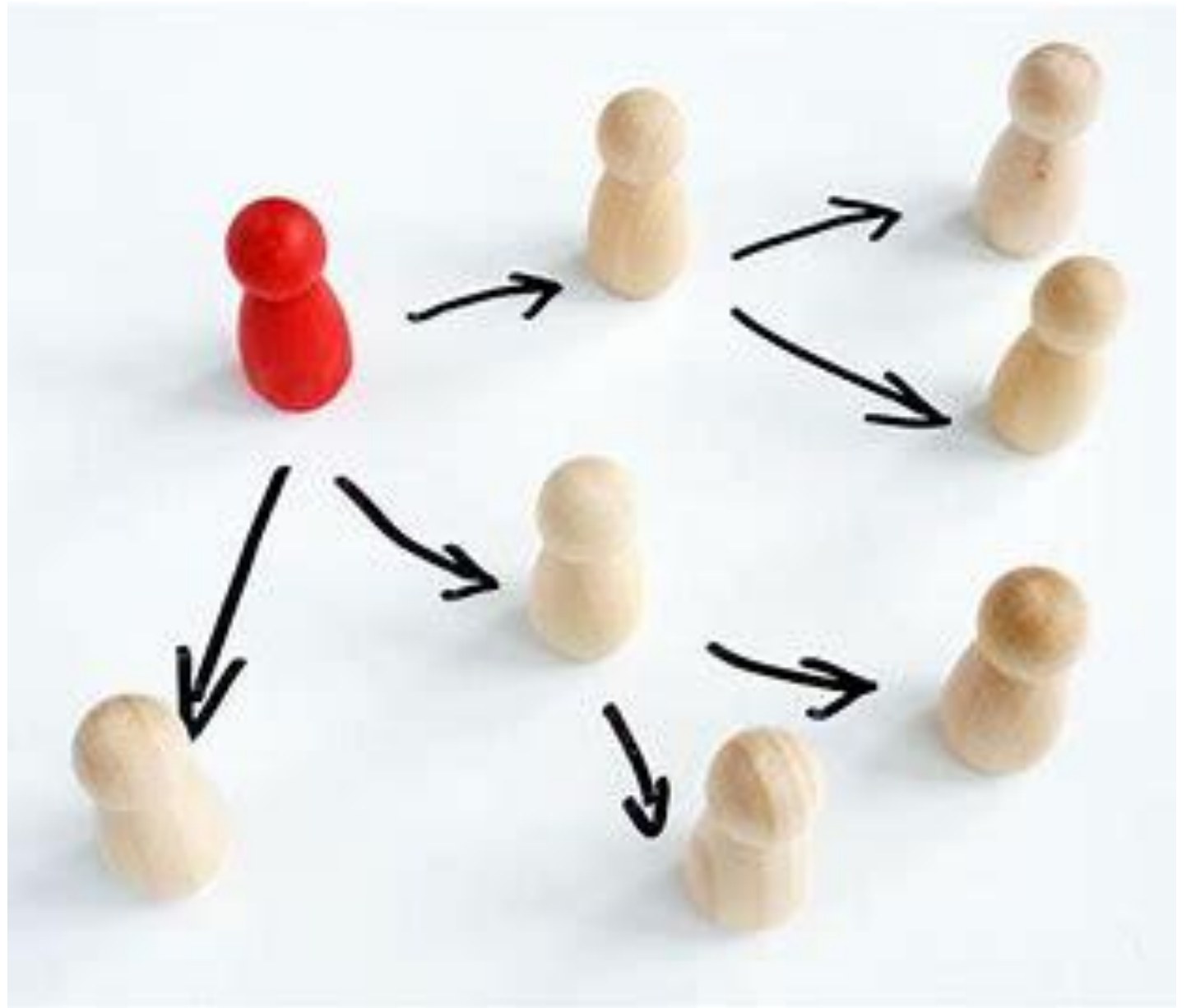
Annex C: Role of the designated safeguarding lead

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. **The designated safeguarding lead should take lead responsibility** for safeguarding and child protection (including online safety and **understanding the filtering** and monitoring systems and processes in place). This should be explicit in the role

DSL role

DSL have lead responsibility for safeguarding and online safety which could include overseeing and acting on:

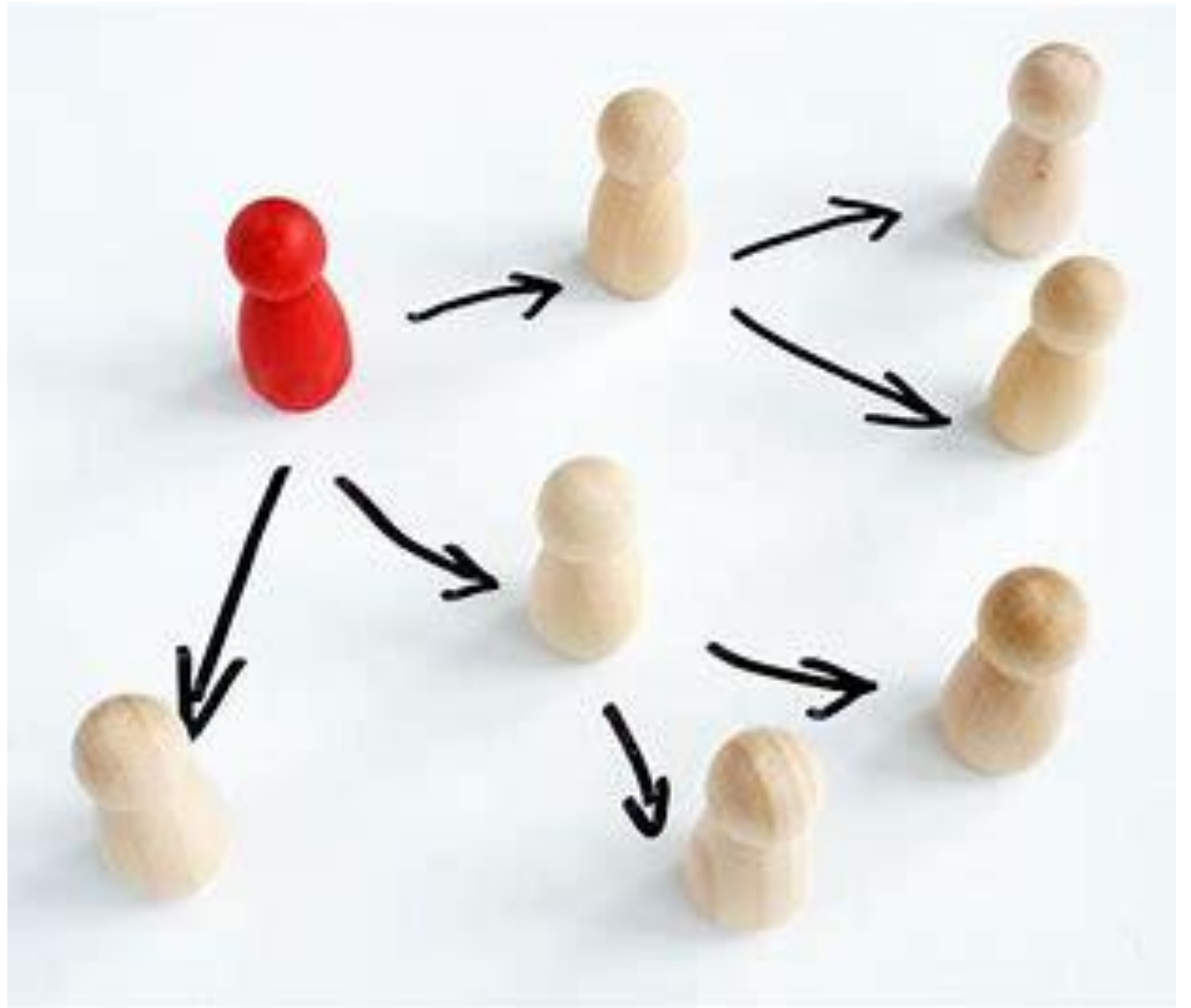
- Filtering and monitoring online reports
- Safeguarding concerns
- Checks to filtering and monitoring systems
- Identified in your JD



IT Provider role

Technical responsibility for:

- Maintaining filtering and monitoring systems
- Providing filtering and monitoring reports
- Completing actions following concerns or checks to the system



All staff should report if:

**ALL
STAFF**



See or suspect unacceptable content accessed



Failure or abuse of the system



Unacceptable content can be accessed



Perceived unreasonable restrictions



Teaching content that could cause a spike in logs



Abbreviations or misspellings that allows access to unacceptable content

You should review your filtering and monitoring provision at least annually

- Risk profile of your pupils
- Current filtering system - why blocked / not blocked
- Specific safeguarding issues, such as county lines
- Relevant safeguarding reports
- Digital resilience of your pupils
- Teaching requirements, for example, your RHSE and PSHE curriculum
- Any specific use case, including Bring Your Own Device (BYOD)
- Related safeguarding or technology policies you have in place
- What checks are currently made and what happens afterwards

**** This should include SLT, DSL, IT provider and Governor**

Mobile devices

Filtering must be working across all devices including mobile devices

What to do

1. Audit devices
2. Ensure apps can be removed centrally and 'routinely'
3. Identify who is responsible for mobile devices (and that the DSL knows who this is)
4. Test. Does filtering work away from the school?
5. Identify any vulnerable learners

What do schools need to do next?

- ✓ Ensure 'Filtering and Monitoring Standards' are met
- ✓ Identify relevant people and allocate roles and responsibilities
- ✓ Ensure that a review group is formed
- ✓ Complete a review and a check of the systems; record this
- ✓ Check mobile devices have centrally administered filtering and monitoring
- ✓ Ensure staff have training about their role, including cyber security

So what do we need to do?

DECIDE:

- Who, how, how often, how actions logged/monitored, how documented, who/where discussed (IT & safeguarding teams)?

FIND OUT:

- Are key things blocked?
- Are we overblocking?
- Is filtering ACTIVE EVERYWHERE (all connections & devices & users)?
- Is Safe Search ENFORCED (can't be turned off) EVERYWHERE (as above)?
- Concerns about students bypassing blocks?

LOG IT ALL!

How can we find those things out?



Ask your tech team to **identify all types of user, device, account and physical location** (remember portacabins, trolleys, home devices, guest networks and BYOD and the most recent new or rebuilt device)

For each one, **document/discuss the following AND ANY ACTIONS:**

- Are expected categories blocked? You could try an obviously but not inappropriate site like guinness.com to show filtering is active (and the alcohol category is blocked).
- Alternatively, if you use LGfL's HomeProtect or SchoolProtect-WebScreen, visit www.hpblock.lgfl.net or <http://www.wsblock.co.uk> respectively (they should NOT load but show a block page – that tells you filtering is active).
- While on the block page, click to see more information and double check you are on the correct policy, e.g. student policy for a student login (if your provider does not have this on the block page, ask how you can test this).
- Check if the expected specific categories are blocked by visiting <http://testwebscreen.co.uk> for WebScreen and www.hptest.lgfl.net for HomeProtect. If your filtering provider doesn't have the equivalent, you can use examples (a gaming, gambling or alcohol website etc, but tell someone first and log this behaviour).
- Check illegal sites are blocked using the Safer Internet Centre's <http://testfiltering.com> (select the green school button then the blue run filtering test button).
- Check YouTube is on one of the two restricted modes via youtubemode.lgfl.net (find out more at youtube.lgfl.net)
- Check Safe Search is on and ENFORCED for all search engines you use (for Google, visit safesearchcheck.lgfl.net and check you can't turn it off)
- Check a site you blocked / unblocked recently or after the last set of checks is correct for all users/accounts/devices.
Remember this may be different for different Key Stages or classroom v office staff for example.

Next, before discussing and considering next steps:

- Ask staff & pupils if they have recently not been able to access educational sites or stumbled across inappropriate sites (and get them un/blocked) and remind them to report promptly in future.

Filtering and monitoring toolkits



[The National Grid for Learning - onlinesafetyaudit \(lgfl.net\)](https://onlinesafetyaudit.lgfl.net)



<https://360safe.org.uk/>

- ▶ A new requirement for ALL governors and trustees to receive, “*appropriate safeguarding and child protection (including online) training at induction.*”
- ▶ **Safeguarding Training for School Governors (free** » [LGfL \(bookinglive.com\)](https://www.lgfl.gov.uk/bookinglive.com)

Filtering and monitoring been in place for a while but now we should be reviewing effectiveness of systems by using out IT, external orgs (buy in IT infrastructure) to help understand patterns and adjust accordingly.

DigiSafe®

Annual School Online Safety Audit & Risk Assessment

CURRICULUM, GENERAL APPROACH & COMMUNICATION

An effective whole school approach requires consistency, a common understanding and clear communication. Unless everyone follows a common approach, you communicate clearly with all stakeholders, and staff know what others are doing, there will be gaps. The same will apply if policies do not reflect practice. And always remember, online safety = online education + safeguarding.

QUESTION	Yes	Partly	No	Notes
<p>Approach: whole school & safeguarding - online</p> <p>- how does the school demonstrate a whole school approach to online safety, as particularly articulated in Keeping Children Safe in Education (KSCE), Teaching Online Safety in School (TOSIS) and subject guidance including Relationships and Sex Education and Health Education (RSE) and Computing?</p> <p>- is online safety fully accepted as part of safeguarding and therefore not treated as a separate matter, in the eyes of staff, students or parents, and equally in the curriculum and communications, or reflected in incident management and staff roles and responsibilities?</p> <p>- are all staff aware that any discussion of online safety, whether planned or ad hoc, may lead to a disclosure and must be dealt with in line with school safeguarding procedures?</p> <p>- is online safety included on safeguarding reports?</p> <p>- does online safety have obvious involvement of the leadership team and governors?</p> <p>- how does the school ensure that non-specialist staff use</p>				<p>2 Evidence / details and dates</p> <p>3 Who is responsible?</p> <p>4 How often is updated?</p> <p>5 How often is updated?</p> <p>6 How often is updated?</p> <p>7 How often is updated?</p> <p>8 How often is updated?</p> <p>9 How often is updated?</p> <p>10 How often is updated?</p> <p>11 How often is updated?</p> <p>12 How often is updated?</p> <p>13 How often is updated?</p> <p>14 How often is updated?</p> <p>15 How often is updated?</p> <p>16 How often is updated?</p> <p>17 How often is updated?</p> <p>18 How often is updated?</p> <p>19 How often is updated?</p> <p>20 How often is updated?</p> <p>21 How often is updated?</p> <p>22 How often is updated?</p> <p>23 How often is updated?</p> <p>24 How often is updated?</p> <p>25 How often is updated?</p> <p>26 How often is updated?</p> <p>27 How often is updated?</p> <p>28 How often is updated?</p> <p>29 How often is updated?</p> <p>30 How often is updated?</p> <p>31 How often is updated?</p> <p>32 How often is updated?</p> <p>33 How often is updated?</p> <p>34 How often is updated?</p> <p>35 How often is updated?</p> <p>36 How often is updated?</p> <p>37 How often is updated?</p> <p>38 How often is updated?</p> <p>39 How often is updated?</p> <p>40 How often is updated?</p> <p>41 How often is updated?</p> <p>42 How often is updated?</p> <p>43 How often is updated?</p> <p>44 How often is updated?</p> <p>45 How often is updated?</p> <p>46 How often is updated?</p> <p>47 How often is updated?</p> <p>48 How often is updated?</p> <p>49 How often is updated?</p> <p>50 How often is updated?</p> <p>51 How often is updated?</p> <p>52 How often is updated?</p> <p>53 How often is updated?</p> <p>54 How often is updated?</p> <p>55 How often is updated?</p> <p>56 How often is updated?</p> <p>57 How often is updated?</p> <p>58 How often is updated?</p> <p>59 How often is updated?</p> <p>60 How often is updated?</p> <p>61 How often is updated?</p> <p>62 How often is updated?</p> <p>63 How often is updated?</p> <p>64 How often is updated?</p> <p>65 How often is updated?</p> <p>66 How often is updated?</p> <p>67 How often is updated?</p> <p>68 How often is updated?</p> <p>69 How often is updated?</p> <p>70 How often is updated?</p> <p>71 How often is updated?</p> <p>72 How often is updated?</p> <p>73 How often is updated?</p> <p>74 How often is updated?</p> <p>75 How often is updated?</p> <p>76 How often is updated?</p> <p>77 How often is updated?</p> <p>78 How often is updated?</p> <p>79 How often is updated?</p> <p>80 How often is updated?</p> <p>81 How often is updated?</p> <p>82 How often is updated?</p> <p>83 How often is updated?</p> <p>84 How often is updated?</p> <p>85 How often is updated?</p> <p>86 How often is updated?</p> <p>87 How often is updated?</p> <p>88 How often is updated?</p> <p>89 How often is updated?</p> <p>90 How often is updated?</p> <p>91 How often is updated?</p> <p>92 How often is updated?</p> <p>93 How often is updated?</p> <p>94 How often is updated?</p> <p>95 How often is updated?</p> <p>96 How often is updated?</p> <p>97 How often is updated?</p> <p>98 How often is updated?</p> <p>99 How often is updated?</p> <p>100 How often is updated?</p>

Digital testing tools

Meeting digital and technology standards in schools and colleges

From: [Department for Education](#)

Published 23 March 2022

Updated: 29 March 2023, [see all updates](#)

In March 2023, the Department for Education published (DfE) new filtering and monitoring standards. Schools need to be meeting these standards straightaway.

Useful links and resources

- [Meeting digital and technology standards in schools and colleges \(DfE\)](#)
- [2023 Appropriate filtering and monitoring definitions published \(UK Safer Internet Centre\)](#)
- [Test Your Internet Filter \(UKSIC / SWGfL\)](#)
- [Filtering provider responses - self-certified by service providers \(UKSIC\)](#)
- [Template Online Risk Assessment \(SWGfL / 360safe\)](#)

Digital resilience

This digital resilience tool is a practical way to assess young people's online behavior and help you make a decision about whether that behavior represents risk of harm.

Behaviors are organized by category and divided into harmful, not harmful, potentially harmful for each age group

Examples of Potentially Harmful Behaviours

0-5 Age group - Gaming alone.

Gaming for the age group is likely to be simple, app-based games on tablets or phones. It's unlikely that a child this age will have the ability to play more complex games on consoles, especially those which require a login process. The main things to consider here are:

- Is the child left alone for long periods with the device? If the child does not have input from anyone else for long periods this could be a concern.
- Is the child easily distracted when other, real world, games are suggested? If so, this is a good sign and suggests no further intervention is needed. If the child is difficult to distract, again the parents/carers may need support around other activities.
- Is the child playing age appropriate games? Violence, sexual content and gambling would be unsuitable. On the other hand, games from Cbeebies are fine for this age group.

6-8 Age group - Ownership of a device

At this age, there are many reasons why a child might have 'own' a device. In some cases children may say a device is theirs when in fact it's a family device, which would then be Not Harmful. In other cases, a parent/carer may buy a mobile phone for a child in case of emergencies. While this should always be possible through the school, club or another adult, it may be that both the parents/carers and child feel less anxious knowing there is a phone nearby.

There are a few things to check if a child suddenly begins talking about their device:

- Parents know about it - if it was given to the child by someone else, without the parents knowledge this would definitely be Harmful.
- Parental controls are set up - parents may need some advice on how to do this, in order to prevent inappropriate content appearing.
- There are appropriate boundaries around the device, such as not having it in the classroom.

9-12 Age group - Online Interaction with strangers

At this age, children may start playing online games and engaging with the online world in new ways. If a child you are supporting says they chat to strangers online you should find out:

- How this interaction happens - did they comment on a Youtube video and have someone to their comment? This would be relatively low risk.
- Are the interactions through games, and if so how much interaction is actually happens? Some games have very limited chat between players whereas others may have long voice calls as part of a campaign. Longer form interaction may be more worrying as children are likely to give more personal details this way, such as which school they go to etc.
- Are parents/carers aware of these interactions and have they spoken to these people? At this age parents/carers should have oversight of these sorts of interactions and would ideally speak to the person the child is interacting with.

13-15 Age group - Regular use of pornography

For young people this age, looking at pornography is not in itself a Harmful behaviour. You might learn about it because the young person talks to you about their concern or because a parent/carer is worried. A few things to consider are:

- How old is the young person? A 13 year old accessing pornography regularly would be more concerning than a 15 year old.
- What does regular mean to them? If a young person always looks at porn while their parents/carers go out to do the weekly shop that might not be too much of concern, whereas if they can't get out of bed in the morning without first watching porn that would be much more worrying.
- What sort of porn is it? Anything violent, extreme or illegal (eg bestiality) would require an intervention.

16-18 Age group - Meeting online friends unsupervised

Young people of this age may have made friends online in a variety of ways and there will therefore be a range of things to consider:

- How long have they known these online friends? If they've been speaking for years and have had video calls there is much less risk of harm. But even if they have met before, it would be best to meet somewhere public.
- What does unsupervised mean? Have they gone with friends (which would be relatively safe) or are they going alone (which would be much more risky)
- Where are they meeting? If they're going somewhere public and have agreed a time to check in with someone or be home it will be much less risky than going to someone's house with no idea when they'll be back.





Guidance

School inspection handbook

Updated 11 July 2022

Safeguarding

343. All schools should have a culture of safeguarding. This means they should have effective arrangements to:

- always act in the best interests of children, pupils and students to protect them online and offline, including when they are receiving remote education

Guidance

Inspecting safeguarding in early years, education and skills

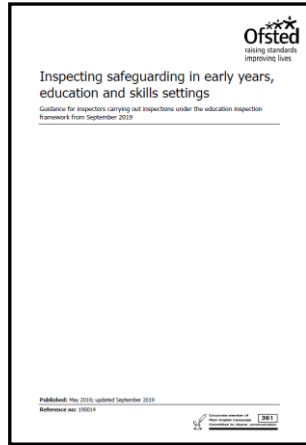
Updated 1 September 2022

Inspecting how effectively leaders and governors create a safeguarding culture in the setting

[...] 25. Inspectors should consider evidence that: [...]

- governing bodies and proprietors do all that they reasonably can to limit children's exposure to any risks from the school or college's IT system. As part of this process, governing bodies and proprietors ensure that their school or college has appropriate filters and monitoring systems in place to protect children from potentially harmful content, and regularly review their effectiveness.

Ofsted



In schools and further education and skills providers, leaders, governors and managers should assume that sexual harassment and online sexual abuse are happening in their setting, even when there are no specific reports.

Adults understand the risks associated with using technology, including social media, of bullying, grooming, exploiting, radicalising or abusing children or learners. They have well-developed strategies in place to keep children and learners safe and to support them to develop their own understanding of these risks and in learning how to keep themselves and others safe. Leaders oversee the safe use of technology when children and learners are in their care.

- Ofsted will explore **child on child abuse** (data and narrative) following the review published in June 2021
- Inspectors will consider evidence on whether governing bodies and proprietors do all they reasonably can to limit **children's exposure to risks through the setting's IT systems.**

[Inspecting safeguarding in early years, education and skills - GOV.UK \(www.gov.uk\) updated](https://www.gov.uk/government/publications/inspecting-safeguarding-in-early-years-education-and-skills-settings) Sept 2022;

Ofsted announced changes in June 2023 to some aspects of its inspection process. From a safeguarding perspective Ofsted have said:

"They will return within 3 months of an inspection report being published, and parents will be informed of this intention in the report. If the school has been able to resolve the safeguarding concerns it is likely to see its overall grade improve. From September we will offer schools greater clarity about the threshold for effective vs. ineffective safeguarding, We will also describe ineffective safeguarding more clearly in inspection reports, to help reassure parents and others that these judgements are not made lightly."

[Changes made to school inspections - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/news/changes-made-to-school-inspections)



Summary

- An overview of the [safeguarding policies and procedures](#) in place
- Whether the policies, procedures and the [single central record](#) are up-to-date and reflect recent changes in legislation
- A sense of whether staff and governors have had all the training they need, including [safer recruitment](#) and [Prevent](#) training
- A sense of the school's safeguarding strengths, incidents and any safeguarding priorities/trends that will be on an action plan over the next year
- Staff may also need to update your school's attendance policy to reflect support around children absent from education and recognise the potential impact of mental health on absence from school.
- Review the DfE's [digital and technology standards](#) to see if your school meets them, and discuss with IT staff/your school's service provider what your school can do to improve. You must complete an **annual online safety audit** to evidence your work.
- Ensure your training for staff on KCSIE 2023, details filtering and monitoring expectations and responsibilities
- Ensure you are informing shortlisted candidates about conducting an online search as part of their recruitment process and include in your safer recruitment policy.