A white background with blue text

Description automatically generatedKeeping Children Safe in Education[[1]](#footnote-2) states that “schools and colleges should consider carrying out an annual review of their approach to online safety”. This should be led by the designated safeguarding lead because they “take lead responsibility for safeguarding and child protection (including online safety and understanding…filtering and monitoring…” (KCSIE 2024).

**Recommendations:**

* **link/integrate this to your overall Section 175 / LA safeguarding audit**
* **use the sections on filtering & monitoring as your annual F&M review**

(saves time but above all ensures an integrated ,whole-school approach)

* **share results with your school governors/trustees**
* **DO NOT ask colleagues to complete the separate sections in isolation and simply paste them together at the end** (mitigates against knowledge transfer and a whole-school approach)

**NEW FOR 2025** – this version of the online safety audit has been updated in various ways but the key things to focus on since the previous version are the updates to the DfE standards in October 2024 and the proliferation of **generative artificial intelligence (gen AI)** tools, whether in regard to school use thereof, filtering and monitoring or covering in the classroom.

The audit is in two broad sections:

* Curriculum, General Approach & Communication
* Safe School Systems (technology for safeguarding and safeguarding for technology)[[2]](#footnote-3)

Whilst the DSL should ‘own’ the audit, it is of course key to involve technical and curriculum colleagues with their distinct expertise, responsibilities and insights. An online safety audit should be a living document, reflecting the realities of technological change, evolving harms and user behaviours. This means for example, the latest national, local and school trends and incidents (which will also be reflected in your training and policies – see the LGfL template OS policy for examples).

We suggest you use the final column to add the evidence, links, details and when it was checked, plus risks and actions/mitigations (by way of documenting your risk assessment – which you may also wish to copy into a separate document depending on your approach).

You may edit this template and add your school logo but please do not remove the LGfL branding or copyright notice. To share this tool with other schools, ask them to visit [onlinesafetyaudit.lgfl.net](https://onlinesafetyaudit.lgfl.net) for the latest version as we will update it through the year.

We welcome feedback and suggestions via [safeguarding@lgfl.net](mailto:safeguarding@lgfl.net)

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 safeguarding = safeguarding*.

| Question | **F**u**lly In Place** | **Partial/ Needs Review** | **Not In Place** | • Evidence/details (e.g. documents, training, reminders) & dates  • Actions / by whom – make these **clear**  • Add colour highlights for items to add to risk register  *NB – we pre-filled some examples / links – delete as appropriate* |
| --- | --- | --- | --- | --- |

|  |
| --- |
| approach |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Approach: whole-school & safeguarding-driven**   * 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, and reflected in incident management and staff roles and responsibilities? * How does the school demonstrate a whole-school approach to online safety, as particularly advocated in Keeping Children Safe in Education (KCSIE), Teaching Online Safety in School (TOSIS) and subject guidance including Relationships and Sex Education and Health Education (RSHE) and Computing? Are all staff aware that any discussion of online safety, planned or ad hoc, by staff or visitors, may lead to a disclosure and must be dealt with in line with school safeguarding procedures? * Is online safety included on safeguarding reports to governors and in safeguarding concern systems – preferably integrated throughout rather than discrete? * Does online safety have obvious involvement of the leadership team and governors? * How does the school ensure that non-specialist staff use consistent approaches and messaging? * Does the school take a non-victim-blaming approach (avoiding statements such as “well you shouldn’t be on social media anyway” in response to an incident or disclosure)? How is this evidenced? |  |  |  | It may be helpful to reference  <https://www.gov.uk/government/publications/teaching-online-safety-in-schools> |
| **Approach: flexible, current curriculum**   * How does the school combine an informed, proactive, planned approach with a flexible, reactive approach to ensure it meets changing pupil needs (e.g. as technology changes, trends develop, incidents occur in school, are they fed into curriculum design and staff training)? * Are staff comfortable with making the most of ad hoc opportunities to discuss and learn as online safety conversations arise? * Are staff empowered to make changes to the scheduling and content of planned lessons to meet neds as they arise throughout the year (e.g. if there is a bullying incident in October, not waiting to teach this until Easter)? * How does the school review annually that teaching is current and relevant to the setting and pupil needs and experiences? * Are all the harms and issues and ‘underpinning behaviours’ mentioned in TOSIS and the RSHE guidance addressed throughout the year? * How are new trends identified and how are these incorporated into the curriculum as needs arise, even during the year (e.g. new gen AI tools and harms)? * Does the curriculum cover the use of emerging AI tools such as nudifying apps, AI girlfriends, etc and recognise that many pupils will come across these at home? * Is particular consideration made for vulnerable students, e.g. those with SEND and other needs? * How does the school avoid overlapping teaching, e.g. covering the same issue in different subjects (e.g. RSHE and Computing)? * Do you collate ‘pupil voice’ to ensure messaging addresses pupils’ lived experiences? * Do curriculum planners meet with safeguarding team to ensure shared awareness of incidents and current needs as well as lesson plans and notable outcomes, strengths and weaknesses? * Do you ensure that positive experiences online are also celebrated (not just harms and negative aspects of life online)? |  |  |  | You may wish to reference/consult:   * <https://www.gov.uk/government/publications/teaching-online-safety-in-schools> * <https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education> * <https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study> |
| **Assessment**   * Is the curriculum informed by and measured against clear outcomes, e.g. those in the UKCIS framework Education for a Connected World (or similar)?How do you use formative and summative assessment to ensure you are aware of pupil knowledge and skills to inform teaching, and subsequently to measure progress |  |  |  | Education for a Connected World is available at [gov.uk/government/publications/education-for-a-connected-world](https://www.gov.uk/government/publications/education-for-a-connected-world)  If other, state here plus links to any schemes of work  The SafeSkills online safety quiz tool is free for all UK schools to use and includes teacher stats [safeskills.lgfl.net](https://safeskills.lgfl.net)  What other assessment tools are in use at your school? Give link/details here |
| **Parental engagement**   * How do you proactively engage parents/carers? * Are parents aware of the school’s broad online-safety approach? * Have you supported parents to become aware of the latest harms and issues as well as encouraged to use safety settings on popular platforms, devices, games, apps and consoles? * Are parents reminded of the importance of following age ratings? * Do you follow a drip-feed approach to communicating with parents? |  |  |  | Resources from [parentsafe.lgfl.net](https://parentsafe.lgfl.net/) may be helpful here and [scare.lgfl.net](https://scare.lgfl.net)  Use our Parent Online Safety training materials to help you deliver sessions to parents in your school: [parentonlinesafety.lgfl.net](https://parentonlinesafety.lgfl.net) |
| **External influences, resources and scares**   * Are external resources always first assessed for appropriateness (age appropriate, not overly negative, scary, victim blaming etc.)?Are any externally purchased schemes of work/curricula carefully adapted as necessary (both proactively at the start of the year and in response to incidents/trends)?What approach does the school take to reacting to online challenges, scares and hoaxes? * How are any external visitors vetted for expertise, appropriateness and safeguarding understanding? |  |  |  | It may be helpful to reference   * [scare.lgfl.net](https://scare.lgfl.net) * [gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes](https://gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes/harmful-online-challenges-and-online-hoaxes) * UKCIS victim-blaming guidance *(soon to be published at time of publication of this document)* * gov.uk/government/publications/using-external-visitors-to-support-online-safety-education-guidance-for-educational-settings   LGfL provides signposting to a range of themed resources at <https://saferesources.lgfl.net> |

|  |
| --- |
| Policies & PRACTICE |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policies**   * Do your policies govern all online behaviour, not just when using school devices or logged into school systems and platforms? * Do you have an online safety policy (whether standalone or section within your safeguarding and child-protection policy)?Do you have (note the following might be integrated into other policies and not standalone but must be very clear if so) * AUPs to reflect varied roles and responsibilities, e.g. different key stages, parents, staff, visitors, governors, contractors etc. (NB whilst often called “acceptable use policy”, these should reflect all online behaviour). * Social media policy? If not, this may be included in your online safety policy but should be clear. * Home/remote learning policy * Information sharing protocols - How is confidential information shared with other stakeholders? Are all documents emailed via a secure system? * How is the use of generative AI captured within your policies |  |  |  | Several organisations provide customisable templates, including LGfL at <https://safepolicies.lgfl.net> |
| **Content & review, policy v. practice**   * Do you consult others to populate your policy, e.g. review templates (LSCP, fellow schools, The Key, LGfL, etc)? * Where you have used content or templates, have you checked it is relevant to your setting, systems and stakeholders and adapted as appropriate? * Do you regularly review these policies (not just the annual governor review but with staff and pupils who can give insights into practicability)? * How do you check that policies are followed and possible to follow (e.g. references to systems which no longer exist, contradictions with other policies, impossible rules like a ban on mobile photography when there are no school cameras but photos are required)? * Are new systems, platforms, processes and user behaviour/needs and incidents regularly embedded into these ‘living’ documents? * Are policies updated to reflect curriculum needs, behaviour and safeguarding risks and incidents in your school? |  |  |  |  |
| **Reporting**   * Is there evidence that staff understand how to report online safety concerns? * Is online safety included on safeguarding reports – preferably integrated throughout rather than discrete? * Are children supported in an age-appropriate/developmentally - appropriate way to tell staff if they have an online safety concern? * Is there evidence that online safety concerns are followed up in an appropriate and timely manner? * Do all staff understand how to report concerns relation to online safety externally? |  |  |  | * Your local Multi-Agency Safeguarding Hub if they have a safeguarding concern about a child. * The [Internet Watch Foundation (IWF)](https://www.iwf.org.uk/en/uk-report/) if settings need to report illegal images. (child sexual abuse material) * The [Child Exploitation and Online Protection centre](https://www.ceop.police.uk/ceop-reporting/) (CEOP) if they are worried about online abuse or the way that someone has been communicating online. * The [UK Safer Internet Centre Helpline for Professionals](https://saferinternet.org.uk/guide-and-resource/need-help#:~:text=Professionals%20online%20safety%20helpline&text=The%20helpline%20can%20be%20contacted,charged%20at%20local%20call%20rate).) |

|  |
| --- |
| Training |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Training & CPD**   * Do all staff receive online safety training as part of the safeguarding training schedule (at induction and start of year or mid-year for new starters)? How does this training reflect the approach you have outlined in this audit? * Is the centre of expertise in online safety within the DSL team, with the most in-depth training available to this team? * How are ALL staff made aware of and regularly updated on national/regional trends and those in school relating to general behaviour, harms or incidents which non-specialist/senior staff may not be aware of without explicit updates * Is training appropriate to and customised for different roles and responsibilities, with extra strategic elements for SLT and governors? * Does training around ‘online safety’ tie in with training on other areas which may not be classically associated with online safety, such as all the harms mentioned in KCSIE (e.g. Prevent and many others)? * Do technical staff receive sufficient training on key safeguarding elements (note particularly filtering and monitoring changes)? * Do non-technical staff receive sufficient training on technical aspects (as above, particular – but not exclusive – focus on filtering and monitoring)? * Have technical, safeguarding, PSHE and other staff been given up to date information on the latest gen AI tools in use (as mentioned above, nudifying apps and nude image generators, AI girlfriends, etc)? |  |  |  | Free training is available from LGfL at [safetraining.lgfl.net](https://safetraining.lgfl.net)  And from most LSCPs (Local Safeguarding children Partnerships)  Excellent paid training is available from many organisations such as NSPCC.  Free quiz for staff on Online Safety also available here: [kcsiequiz.lgfl.net](https://kcsiequiz.lgfl.net)  **Trends nationally are outlined in the LGfL template policy (see** [**safepolicies.lgfl.net**](https://safepolicies.lgfl.net)**)**  Your school trends should be documented too |

[ END OF SECTION 1 ]

Safe School Systems

Schools have a duty to provide safe school systems – this may take the form of technology for safeguarding (e.g. filtering and monitoring) or safeguarding for technology (such as the safest settings on a particular device or platform), as well as the relevant behaviours.

It is important to remember that technology changes all the time, whether functionality, risks or appropriate settings, hence this section needs a thorough review each time you look at it. There is always a balance to be struck between safety precautions and ‘over-blocking’, which Keeping Children Safe in Education requires schools to avoid for filtering, but which is also relevant when you consider if a system is so locked down that it interferes with teaching and learning. The education element is therefore key, i.e. teaching children and young people what to do when they see or experience something worrying.

Safeguarding teams will wish to engage with their technical colleagues on this section – please ensure to review it together.

| Question | **F**u**lly In Place** | **Partial/ Needs Review** | **Not In Place** | • Evidence/details (e.g. documents, training, reminders) & dates  • Actions / by whom – make these **clear**  • Add colour highlights for items to add to risk register  *NB – we pre-filled some examples / links – delete as appropriate* |
| --- | --- | --- | --- | --- |
| FILTERING | | | | |
| **General – a high-quality and school-appropriate filtering service**   * Has your provider filed a submission with the UK Safer Internet Centre to explain why your filtering is appropriate? * Have DSL, SLT and technical teams all read and understood the submission, including rationale, benefits and limitations and safe search settings, e.g. for web searches and YouTube? * How do you know your provider goes above and beyond this (e.g. with independent accreditation; if not, what other checks have you done to be sure the provider meets its obligations? * How do you know that you are using best-practice settings for your system? |  |  |  | LGfL’s UK SIC submission is linked to at the bottom of [safefiltering.lgfl.net](https://safefiltering.lgfl.net) (delete as appropriate).  Safer Internet Centre submissions for LGfL and all other providers - [saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/filtering-provider-responses](https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/filtering-provider-responses)  YouTube guidance (incl mode check) - [youtube.lgfl.net](https://youtube.lgfl.net)  Google safe search check - [safesearchcheck.lgfl.net](https://safesearchcheck.lgfl.net)  Accredited school filtering providers are here:  [saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering/filtering-accreditation-scheme-for-uk-schools](https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering/filtering-accreditation-scheme-for-uk-schools) |
| **General – knowledge, approach, attitudes**   * How do you ensure there is a general understanding of the following (verbatim from the DfE standards introduction)?   + “Filtering is preventative […] protect[s] users from accessing illegal, inappropriate and potentially harmful content […] identifying and blocking specific web links and web content”   + “No filtering system can be 100% effective. […] You need to understand: your filtering system’s coverage [and] any limitations” * How does the DSL team maintain a knowledge in general terms of WHAT is blocked (or allowed), for WHOM, WHEN/WHERE and most importantly WHY (safeguarding not tech-driven rationale)? * How are all staff reminded that filtering is all about safeguarding and that they are the eyes and ears to warn of gaps or overblocking? * Is the DSL team clearly in charge of filtering (not the same thing as being technical experts or ‘doing’ configuration/setup)? * Are you confident you follow best-practice recommendations, e.g. to be as granular as possible (using user authentication and decryption)? |  |  |  | Note here how you achieve this and how you check/reinforce  e.g. your training schedule/content  Some best-practice tips are here: [filteringtoptips.lgfl.net](https://filteringtoptips.lgfl.net) / [safefiltering.lgfl.net](https://safefiltering.lgfl.net) |
| **DfE Standards – high level**   * Do DSLs and SLT understand that they are not complying with the standards by subscribing to a reputable filtering providers, but that compliance is based on how/whether a school uses filtering appropriately for its setting, and on the rationale for decisions and day-to-day practice by the school? * At a very high level (detail to follow), are you satisfied your school is complying with these standards (NB this section relates mostly to S1-3)? * What are the key action areas for the school to improve on and improve compliance over the next 12 months? |  |  |  | Find the standards at <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges> |
| **Standard #1 - Identify and assign roles and responsibilities to manage your filtering and monitoring systems**   * Where are these roles / responsibilities outlined (normally online safety policy and maybe AUPs too) * How do you ensure that the DSL and IT teams collaborate effectively to make informed, decisions (details of how/when)? * How often does the DSL team check reports, what do they check and how do they track actions? * Who is your named F/M governor and SLT member (DSL is the lead but some may have additional SLT support)? * How do they understand their roles and are all staff aware who they are and their roles? * What is the mechanism and schedule for involving / feeding back to governors/SLT on regular checks and reviews? * Who are the internal and/or external technical support (setup, configuration, operation), and are they and all staff aware of them and their duties? |  |  |  | Free templates for online safety policies and AUPs which can be used by any school in the country are at [safepolicies.lgfl.net](https://safepolicies.lgfl.net)  Note also video for governors on filtering at [safefiltering.lgfl.net](https://safefiltering.lgfl.net)  For LGfL schools, the new reporting dashboard with search term word cloud, category pie charts and real time data analysis may be helpful. |
| **Standard #2 - Review your filtering and monitoring provision at least annually**   * Where and how is your annual review carried out and documented (this section of this document is intended to be used as your review if you so wish)? * Who is present for this review, where are results logged and how are actions followed up on? * Is the provision safeguarding-driven, rather than based on convenience or ‘how it always was’? * Is there sufficient technical input to be realistic and well informed, and sufficient safeguarding input that decisions are based on the best way to keep children safe and teach effectively? * Has care been given not to be too restrictive and ‘overblock’ by impacting teaching and learning, by removing so much risk that pupils do not learn about the risk online they would face at home or sex education terms are blocked? * Are systems in place to identify if a review is needed more than annually (e.g. if there has been a significant change)? * How is your review informed by the latest trends nationally and in school? * How are outcomes of the review communicated with all staff? * How are ‘regular checks’ carried out, by whom and how often; where are these checks documents; how are the results fed back to the DSL and actions decided/followed up on? * Do checks cover these questions: * Are the key things still blocked/allowed as we need/think they are? * Are we overblocking in any way? Is filtering ACTIVE EVERYWHERE (all connections & devices & users)? * Is Safe Search ENFORCED (can't be turned off) EVERYWHERE (as above)? * Is the YouTube mode enforced as expected? * Are there concerns about students bypassing blocks? * Have we asked staff for feedback? |  |  |  | You might choose to log your results here to start a new online safety audit each time, or to log it elsewhere.  It might make sense for the regular checks to include whether or not a new review is needed mid year due to changes. There is a template for regular checks (different to this document) at [safefiltering.lgfl.net](https://safefiltering.lgfl.net)  You may want to use our Filtering Checks template, available to download for free [safefiltering.lgfl.net](https://safefiltering.lgfl.net) |
| **Standard #3** **- Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning**   * What does your system block/allow, for whom, where (eg home v school) and most importantly why? (NB you could either include this here or a link to an external document) * How is it flexible depending on context (e.g. what is allowed for older pupils only or with risk mitigations)? NB – the DfE standards state that a different staff and student policy is a minimum; best-practice is seen as much more granular. * Where do you deviate from the recommendations of your provider and/or other expert advisers, and WHY? What are the mitigations? * How does this support your current setting/cohort, their needs and recent safeguarding harms and trends? * What have you changed in the past year to improve the system? * What have you changed in the past year in response to safeguarding / behaviour / PHSE team input? * How are pupils taught to manage risk and allowed access to more content as they grow older? * What is your approach to generative AI sites (which can generate useful images/text/videos but also highly sexualised content, encourage self-harm or other inappropriate items)? * Are you only using gen AI websites that meet the Jan 25 DfE ‘[Generative AI: product safety expectations](https://www.gov.uk/government/publications/generative-ai-product-safety-expectations/generative-ai-product-safety-expectations)’ and with regard to DfE document ‘[Generative artificial intelligence (AI) in education](https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education)’? * Search engine/s: * Which do you allow and are all others blocked? * Do these allow safe search to be enforced? * Do these have embedded AI responses/if so how is this age appropriate? * Is the above covered in your regular checks schedule? * Which YouTube restricted mode do you use, why and how is it regularly checked? * Is effective RSHE possible insofar as pupils can access sex education and safely search for correct anatomical words? * Does your provider block the relevant illegal content lists (check their submission to UK SIC)? These are CTIRU, IWF, PIPCU. * Do teachers regularly confirm that teaching and learning is not impacted by overblocking, and the risk balance is correct and pupils confirm that they are learning about managing risk online in lessons and ad hoc opportunities? * Do students confirm that using devices at school helps them manage this on private devices at home? * Are staff, pupils and parents reminded that the internet can never be 100% safe and things will go wrong but as a school we will learn from it and improve, always provide a much safer environment than at home and empower school staff to use times when things go wrong as teachable moments? |  |  |  | Detail how this links to current risk  Re who/when etc e.g. times of day might be different such as gaming only at lunchtime, social media only in the staffroom, less strict for older pupils or photo sites for photography students, safe search engines for the very youngest etc  More info at <https://youtube.lgfl.net>  Check safe search status via [https://safesearchcheck.lgfl.net](https://safesearchcheck.lgfl.net/)  See how LGfL filtering is appropriate via [appropriate.lgfl.net](https://appropriate.lgfl.net) (scroll to bottom) and for others via UK Safer Internet Centre website |
| **Standard #4 - Have effective monitoring strategies that meet the safeguarding needs of your school or college**  ***NB - This standard is mainly about monitoring, not filtering. Please ensure you are aware of the difference (see intro to DfE Standards); but when it comes to checking reports/logs for your filtering, you may wish to consider these points:***   * Which regular reports are run and on what? What is the purpose of these checks, what is looked for? * Who checks logs and how does this happen when there is an incident that needs investigating? * Can you report on what students search for (NB this requires decryption)? * How has your system been changed over the past year to make it safer or more appropriate in other ways? * Do logs and reports from your system enable you to identify users – where this is not possible, what risk mitigations do you have in place (e.g. stricter filtering if you cannot tell the user) or manual ways of logging users (e.g. if a set of ipads cannot be tracked to a user, note on paper who was issued each device)? * How does what you do here tie in with any technical monitoring system you may have (given that most of Standard 4 relates to dedicated monitoring systems)? |  |  |  | Give name and system/login – best to have multiple people able to do this and not just external support  These reports might normally only be run at the time of your ‘regular checks’ e.g. half-termly. How often do you do this, who carries it out / helps the DSL analyse/next steps etc.  And WHICH reports are run? E.g. top blocked / top allowed categories and top blocked / top allowed sites?  State your approach to search terms, how these are examined, if autocomplete is disabled to help you see real searches, etc  For LGfL schools, in addition to reports how do you use the reporting dashboard with near real time stats? |
| **Filtering training**   * Has your technical team attended training on your filtering platform/s to understand exactly how it works, how it is set up and what the options are in order to inform a strategic filtering approach and implement DSL/SLT requirements? * Has your safeguarding team also attended training to know the questions they need to ask of their technical colleagues and to understand at a high level what filtering can/should do to inform the approach? * Are both technical and safeguarding colleagues taught that when content is blocked but required for access, it is best practice to allow the site rather than the entire category? * Is there an awareness of the wide-range of content in categories such as shopping (even the most popular shopping site sells sex toys) and entertainment (which would include the latest from Strictly but also explicit discussion of sex and other adult themes in the same way these might come up on television)? * Have you included F&M in your start of year safeguarding briefing and/or other insets to ensure all staff are aware of the importance of this area, that the DSL team drive strategy, and that they are the eyes and ears to pass on gaps or overblocking? |  |  |  | Tech training - <https://lgfl.bookinglive.com/book/add/p/23>  Safeguarding training (30 minute overview of filtering) - <https://lgfl.bookinglive.com/book/add/p/5> |
| **Rationale / team effort**   * Do your technical and safeguarding teams meet to discuss your filtering needs and document your approach regarding what is allowed / not in school and the safeguarding-driven rationale? * Is this up to date, reflected accurately (and updated) in policies and practice, including how your approach and settings do not ‘over-block’, and shared with parents, staff and governors and ready to show to Ofsted? |  |  |  |  |
| **BYOD**   * If you allow ‘bring your own device’, what measures are applied to these devices to ensure the school internet cannot be used inappropriately simply by switching to a BYOD? network |  |  |  | NB there are many different approaches – some schools do not allow BYOD; many do or restrict it to certain groups. Some schools insist upon logging in if using the BYOD network; others where this is not possible might choose to make it much more restrictive |
| **Devices at home**   * Have you applied filtering to school devices when sent home with students? * Given that schools cannot protect parent/child devices, do you remind parents about how to set controls on their home internet/phones/devices etc? |  |  |  | Web filtering for school devices at home is available from various providers including LGfL [homeprotect.lgfl.net](https://homeprotect.lgfl.net) – those solutions which also have Chrome extensions can also protect children if they access a school profile on a family device  See <https://parentsafe.lgfl.net> for support with parental control settings and other ways parents can keep their children safe online |
| **Linked to the curriculum and safeguarding landscape**   * Is your filtering set up and updated to reflect the online-safety messages you teach and safeguarding concerns/cases in school? * Conversely, is learning from filtering findings used to inform the curriculum? |  |  |  | An example for Q2 in this row – if there is a spike in failed attempts to view pornographic sites, is this covered in class as a priority, regardless of where it may fall in the scheme of work / plan for the year? |
| MONITORING   * Note you may wish to merge the filtering and monitoring sections, especially if they are from the same provider. * However please note that filtering & monitoring are distinct – [safefiltering.lgfl.net](HTTPS://SAFEFILTERING.LGFL.NET) has a video to explainer and the introduction paragraph to the dfe standards also covers the differences. | | | | |
| **(Note previous section covers monitoring as well in all the other standards in terms of roles, reviews, etc and this section focuses on Standard 4)**  **DfE Standard 4 and Monitoring Approach**   * Are you satisfied that overall your school is complying with standard #4 “You should have effective monitoring strategies that meet the safeguarding needs of your school or college”? * What are the key action areas for the school to improve on and improve compliance over the next 12 months? * How are all staff helped to understand the difference between filtering and monitoring? Do they understand these two sections (verbatim from DfE Standards): * “Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity […] solutions do not block users from seeing or doing anything.” * Are monitoring captures dealt with by the safeguarding team (not technical staff)? Who does what? * How does the safeguarding team find the time to deal with captures (do you have a human monitoring service that also looks at captures / are others supporting the team – if so are they safeguarding trained and aware of current trends)? * Is your approach to monitoring based on a strategic and safeguarding-driven rationale that has been made in discussion between safeguarding and technical teams? * Which of the four monitoring strategies listed in the DfE standards do you use, where and why? * Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. * Technical monitoring solutions rely on software applied to a device that views a user’s activity. * Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. * Are all senior leaders, governors and staff aware of this rationale and which approaches are used where? * How is the system updated in line with the latest concerns around issues or users, new flags or keywords etc added? * Beyond the captures flagged immediately or daily, who uses the system to look for trends and compare with other systems? What is the methodology for this? * How are results from monitoring fed into the safeguarding reporting systems (e.g. CPOMS/myConcern) to ensure the ‘safeguarding jigsaw’ is not fragmented? |  |  |  | You may have used the video on the differences between F/M at [safefiltering.lgfl.net](https://safefiltering.lgfl.net)  Standard 4 on this page lists these options and what you should do - <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges>  Safer Internet Centre monitoring guide and options - <https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring> |
| **Appropriate monitoring**   * If you use a pro/active technical monitoring solution, has the provider filed a submission to the UK Safer Internet Centre? * Have DSL, SLT and technical teams all read and understood this submission, including rationale, benefits and limitations? * Have you satisfied yourself that your filtering provider meets the items on the checklist offered by the Safer Internet Centre? * How does monitoring respond to but also feed into the curriculum (e.g. lots of captures on issue X might lead to lessons being reordered) and into proactive safeguarding interventions for whole groups? |  |  |  | Safer Internet Centre appropriate monitoring provider submissions – [saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/monitoring-providers-responses](https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/monitoring-providers-responses)  Statement for filtering in general - [saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring](https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring) |
| **Limitations**   * With most providers there will be some activity that cannot be viewed, or instances where it is much more difficult to track who is using a device. What are these limitations and what mitigations (e.g. more restrictive access) or manual controls (e.g. a physical log of who uses which ipad in a lesson) are in place? * Are staff aware of whether keywords only are monitored, if these are set in context, whether images are screened or not, whether context can be given etc. * What is in place for devices in the home and BYOD if applicable? * What physical / real time monitoring of screens takes place, when and how (e.g. a teacher walking around and watching screens, or some schools have a live view of a whole class set of screens etc)?How do you avoid too many false positives making the system unusable? * How are staff encouraged to help the team by flagging if they are planning e.g. a lesson that will bring lots of flags (e.g. a poem that mentions death or suicide, research into wars or an RSHE lesson on sex or intimate body parts etc)? |  |  |  | E.g. Mobile devices, especially iPads, are frequently much harder to monitor outside the browser; apps which are not web based can often not be monitored, some devices are not set up with per-user logins  If you have a classroom management tool, state how it is used and/or how teachers use their physical presence |
| **Monitoring training**   * If using a pro/active solution, has your technical team attended training to understand exactly how it works, how it is set up and what the options are in order to inform a strategic approach and implement DSL/SLT requirements? * Has your safeguarding team attended training to know the questions they need to ask of their technical colleagues and to understand at a high level what monitoring can/should do to inform the approach? |  |  |  |  |
| **System configuration, customisation and review**   * Do your technical and safeguarding teams meet to discuss your monitoring needs and ensure systems are configured for the devices and systems you used and regularly updated/reviewed where changes are made and new devices added to ensure no devices or systems are missed? * How does the annual review and regular checks feed into settings and issues looked for on the monitoring system? This includes safeguarding teams requesting new items (e.g. keywords, particular users) to be added for flagging when mentioned or to see all activity responding to concerns, trends or incidents? * Are systems customised for your safeguarding needs – e.g. adding keywords that represent new concerns in your school/area or to follow students at particular risk. Is this approach documented and the system regularly reviewed to ensure appropriate access, settings and usage / do your policies reflect practice in school and are they updated when settings / approach are changed? |  |  |  |  |
| **Reports**   * If using a pro/active solution, is the system set up in such a way that you have a manageable number of captures and are not overwhelmed and therefore at risk of missing key safeguarding alerts? * Do you also run reports to spot trends over time? * Are concerns fed into the safeguarding systems you use to capture manual/offline safeguarding concerns to complete the safeguarding jigsaw and not kept in a separate silo? |  |  |  |  |
| **Other**   * Please also consider the school devices when at-home / curriculum / BYOD questions mentioned in the filtering section above and add any aspects not already covered there. |  |  |  |  |
| HOME / REMOTE LEARNING & DEVICES IN THE HOME | | | | |
| **School devices in the home**   * If you send school devices home with students, how are they protected / monitored? * Do you have internet filtering/monitoring on them? (NB the standards stress that checks for filtering & monitoring should include those used off site)? * Many schools will have less restrictive filtering at home – detail this here and how decisions were made/mitigations? * Are they locked down as ‘managed devices’ or equivalent, so software cannot be un/installed except by school admins? |  |  |  | Web filtering for school devices at home is available from various providers including LGfL. If you use one, list it here.  What about cybersecurity such as antivirus etc? |
| **Live lessons** (most schools deliver scheduled and unexpected live lessons (e.g. open days, elections, snow days, broken boilers, etc.)   * Do you have a home/remote learning policy or clause in another policy that covers behaviour for pupils and staff? * What key safeguarding precautions are included? * Where are they logged? |  |  |  | The infographic at [remotesafe.lgfl.net](https://remotesafe.lgfl.net) has 20 safeguarding considerations for lesson livestreaming that are good precautions to have in place. Whether you use that list or not, note your high-level precautions here. |
| **Homework / cloud platforms accessible from home** (all other platforms that can be accessed at home, whether for homework or during home learning)   * Are these covered in policies and AUPs and regularly updated as new platforms/systems are bought? * Are all systems audited to ensure that they have an audit trail, central administration not limited to one person, oversight of administrators and settings locked down where features are not required, e.g. to not allow unmonitored communications? |  |  |  |  |
| general – ALL TECHNOLOGY USED IN / BY THE SCHOOL | | | | |
| **Safeguarding & technical collaboration and review**   * Do safeguarding and technical teams review at least annually (or whenever significant changes are made to technology or the way the school works or new technologies are adopted), which platforms, systems and devices are used, how, what their settings allow and why, plus risks and mitigations? NB-not just filtering/monitoring. * Are generative AI tools covered in this? What is allowed/not/by whom/when and why? What are the risks and mitigations? * When you do your ‘regular checks’ of filtering/monitoring (we recommend half termly, which other systems are checked/reported on at the same time by IT teams to senior leaders / DSLs? * In 2025 are you paying particular attention to any software (not just websites) which may give access to generative AI tools? Do these meet the Jan 25 DfE ‘[Generative AI: product safety expectations](https://www.gov.uk/government/publications/generative-ai-product-safety-expectations/generative-ai-product-safety-expectations)’ and do you have regard to DfE document ‘[Generative artificial intelligence (AI) in education](https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education)’? |  |  |  | State here where this review document is kept and its latest update / key actions etc and/or which other systems are incorporated |
| **Communication functionality**   * Have you identified all platforms allowed for use in school which have a chat function e.g. Scratch, Bandlab, etc? Have you enforced any safety controls related to these? * Are all platforms that include any chat function (remember that ‘comments’ can be used to chat, especially if they are never monitored) included in your policies, AUPs and risk assessments and locked down in the way your school wants them?   **NB – any gen AI site may have this functionality**   * Are all staff and pupils aware which platforms they can use to communicate between pupils or between staff and pupils and that they must never use accounts/emails/apps that are not approved/linked to the school? |  |  |  |  |
| **Technology in your policies / AUPs**   * Are the latest school system, platforms and devices that **CAN** be used/accessed at home included in your policies/AUPs etc? * Have these been updated/audited recently to ensure they are still accurate? * Are the rules possible to follow (e.g. systems named which no longer exist or “use a school camera” when they don’t exist or work)? * Where is your photo/video policy stored? When was it last updated? * What is your approach to checking the setting’s devices regularly to ensure imagery and content is appropriate? Who does this? How often? What do they check? Do you check/ clear the photo gallery/ camera roll? |  |  |  | See [safepolicies.lgfl.net](https://safepolicies.lgfl.net) for template policies  Consider asking staff and students what they think of policies, not just if they agree |
| cybersecurity | | | | |
| **Audit** **, documentation** **and standards** (given its importance for continuity of access to systems and data for keeping children safe, schools secure and maintaining continuity of teaching & learning, cybersecurity should be audited separately)   * Does your school have the 3 documents recommended by the National Cyber Security Centre? * cybersecurity policy * risk + asset registers * incident response plan * Are these accurate and regularly updated, read by all and reflected in practice? |  |  |  | Info for schools from NCSC: <https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools>  Templates for these three documents including notes to explain to a non-technical audience are at <https://elevate.lgfl.net> |
| **Standards**  Are you aware of and meeting the Cyber Security standards for Schools and Colleges published by the DfE (updated in 2024), which are referred to in KCSIE 2024? |  |  |  | See the standards here <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges>  Template Security Audit and Checks are available at <https://elevate.lgfl.net>  Note here where you document your response to these standards / how you evidence meeting them. |
| **Technical staff**   * Do technical staff have training on cybersecurity and report to senior leaders and governors on issues, mitigations incidents and training needs? |  |  |  | The NCSC questions for governors document may be helpful here – [ncsc.gov.uk/information/school-governor-questions](https://ncsc.gov.uk/information/school-governor-questions) |
| **Training**   * Are non-technical staff given training and regular reminders on cybersecurity best-practice (passwords, phishing, reporting and more)? * Are students taught about cyber security and how to keep their accounts and data safe? |  |  |  | NCSC non-technical training for school staff is available for free, e.g. from LGfL <https://booking.lgfl.net/book/add/p/33>  Training is also available for governors here: <https://lgfl.bookinglive.com/book/add/p/160>  The NCSC also have resources available here: <https://www.ncsc.gov.uk/information/resources-for-schools> |
| DATA PROTECTION |  |  |  |  |
| * Do you have a clear data protection policy in place that meets requirements regarding UK GDPR? * Who is your Data Protection Officer in your setting? * If you have CCTV, is there a robust policy that ensures you comply with data protection legislation? * Who has access to the recordings from CCTV? How is this managed to safeguard children? * As well as the many other considerations regarding generative AI tools, how/where have you made clear to staff what they are/are not allowed to do with school/staff/student data and what they are allowed to use gen AI tools for or not from a data protection perspective? |  |  |  | Information Commissioners Office (ICO): information around data protection and GDPR - <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>  DfE Data Protection Toolkit for Schools: For information on what schools need to do in order to comply with data protection regulations - [www.gov.uk/government/publications/data-protection-toolkit-for-schools](http://www.gov.uk/government/publications/data-protection-toolkit-for-schools) |

1. <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2> [↑](#footnote-ref-2)
2. The ‘Safe School Systems’ section is deliberately more detailed – not to express greater importance but to help non-technical colleagues better understand technical issues via more detail. [↑](#footnote-ref-3)