**This tool is for non-school-based nurseries, playgroups, childminders & creches. Early years settings in schools should use the** [**Online Safety Audit for schools**](https://onlinesafetyaudit.lgfl.net).

With increasing numbers of children reportedly owning and accessing digital media in their earliest years (an [Ofcom report](https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2024) highlighted that 25% of children aged 3-4 yrs **own** a smartphone and 85% go online), it is imperative that early years settings have a proactive and holistic approach to keeping children safe online in their settings, and support parents to do so at home. This audit can help early years settings to review their online safety provision, policies and practice, to evidence good practice and identify any areas for development.

We have created a separate online safety audit for early years settings in recognition that use of digital technology in early years settings can look different to that in school-based settings, and that the guidance for settings also differs.

It is vital this audit is neither treated as a tick box exercise, nor viewed as a static report: it should be a living document that reflects the fluid realities of technological change, evolving harms and user behaviours. This means for example, the latest national, local trends and incidents which will be reflected in your training and policies (see the LGfL [template online safety policy](https://safepolicies.lgfl.net) for national trends we have identified over the past year).

We recommend that this audit should be carried out and reviewed by the Designated Safeguarding Lead annually. Stakeholders (staff, parents and trustees etc.) should be involved in this process and be familiar with the outcomes.

We also recommend that results, conclusions and actions are incorporated into the setting’s overall safeguarding audit/review and considered as part of a holistic approach – not treated separately to offline safeguarding issues.

This audit has been broken down into two broad sections:

* Approach, Learning & Communication
* Safe Systems (technology for safeguarding and safeguarding for technology)

We suggest you use the final column to add evidence, details and when it was checked, plus risks and actions/mitigations to highlight the setting’s strengths and areas of development.

Feel free to edit this template and add your setting logo but please do not remove the LGfL branding or copyright notice. Rather than share the file, copies can be found by visiting [eysafe.lgfl.net](https://eysafe.lgfl.net/)

We welcome feedback to help us improve the tool via [safeguarding@lgfl.net](mailto:safeguarding@lgfl.net).

Please also download our free [Policy Guide for Digital Media Use and Online Safeguarding in Early Years Settings](https://eysafe.lgfl.net/), including a 10-point charter (see below).

Early Years settings are advised to follow the [UK Council for Internet Safety’s advice](https://assets.publishing.service.gov.uk/media/61377fc8d3bf7f05b166a532/UKCIS_Early_Years_Online_Safety_Considerations_for_Managers.pdf) around online safety, as well as the [Internet Safety guidance](https://help-for-early-years-providers.education.gov.uk/safeguarding-and-welfare/internet-safety) outlined by Department for Education.

[A poster of a family

AI-generated content may be incorrect.](https://eysafe.lgfl.net/)

Approach, Learning & Communication

An effective approach requires consistency, a collective 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  • Any actions / by whom – highlight somehow  *NB – we pre-filled examples / links – delete as appropriate* |
| --- | --- | --- | --- | --- |

|  |
| --- |
| 1. approach |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Approach: whole-setting & safeguarding-driven**   * How and why is digital media used within the setting? Is there a clear approach that considers the purpose and consideration for using digital media linked to the early learning goals? * Is online safety fully accepted as part of safeguarding and therefore not treated as a separate matter, in the eyes of staff and parents, and equally in the curriculum and communications, or reflected in incident management and staff roles and responsibilities? * How does the setting demonstrate a whole-setting approach to online safety? * 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 safeguarding procedures? * Does online safety have obvious involvement of the leadership team, committee members and/or trustees? |  |  |  | FREE Policy Guide for Online Safeguarding and Digital Media Use in Early Years Settings – <https://eysafe.lgfl.net>  WHO Guidance on screentime in early years - <https://www.who.int/news/item/24-04-2019-to-grow-up-healthy-children-need-to-sit-less-and-play-more>  Tiny Happy People guidance - <https://www.bbc.co.uk/tiny-happy-people/screen-time-advice>  Internet Matters preschool guidance - <https://www.internetmatters.org/advice/0-5/> |
| **Approach: flexible & current curriculum**   * How does the setting combine an informed, proactive, planned approach with a flexible, reactive approach to ensure it meets children’s changing needs (e.g. as technology changes, trends develop, incidents occur in the setting or in the community, are they fed into the children’s learning and staff training)? * Does your setting use [Education for a Connected World](https://assets.publishing.service.gov.uk/media/5efa05b4e90e075c5492d58c/UKCIS_Education_for_a_Connected_World_.pdf) to shape children’s learning? * Are staff comfortable with making the most of ad hoc opportunities to discuss and learn as online safety conversations arise with children or parents? * How does the setting review that teaching and learning is current and relevant to the setting and children’s needs and experiences? * Is consideration made for supporting vulnerable children, e.g. those with SEND and other needs, to access online safety teaching? * Do you speak to children to understand their experiences of using digital media at home, and take this into account when planning for learning? * Do you ensure that positive experiences online are also celebrated and shared with the team and parents (not just harms and negative aspects of life online)? * Are apps/games/websites/online tools checked for appropriateness by the setting’s management team prior to use? What is your process for this? |  |  |  | Education for a Connected World is a helpful framework that describes the knowledge, understanding and skills that children and should have the opportunity to develop at different ages and stages. This framework includes children aged 4yrs and above. Settings should consider how they provide opportunities to help children acquire these skills and knowledge - [gov.uk/government/publications/education-for-a-connected-world](https://www.gov.uk/government/publications/education-for-a-connected-world)  Common Sense Media’s Digital Citizenship curriculum for early years: <https://www.commonsense.org/education/collections/digital-citizenship-for-early-years-and-primary-learners-uk>  Look at our resources on Online Safety and search by EYFS – <https://saferesources.lgfl.net> |
| **Parental engagement**   * How do you proactively engage parents/carers? * Have you talked to parents about their use of digital media at home and identified what support they may need? * Have you supported parents to be aware of the setting’s online safety approach? * Have you supported parents to be aware of the latest harms and issues as well as encouraged them to use safety settings on popular platforms, devices, games, apps and consoles? * Do you follow a drip-feed approach to communicating with parents? * Are parents signposted to age and stage appropriate programmes/games which support their child’s current interests and stage of development? * Is advice about a balanced approach to device use shared with parents and guidance given? * Do you have a robust approach to seeking and following parental consent about using children’s images in your setting? |  |  |  | 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](https://parentonlinesafety.lgfl.net) to help you deliver sessions to parents in your school: parentonlinesafety.lgfl.net  Digital 5 a Day - <https://www.google.com/url?q=https%3A%2F%2Fwww.childrenscommissioner.gov.uk%2Fdigital%2F5-a-day%2F&sa=D&sntz=1&usg=AOvVaw2YKHlJMr6cpxyLVlj3Rkhs>  Digital 5 a Day poster - https://viewonline.lgfl.net/hubfs/SafeguardED/Posters/LGfL-SafeguardED-Poster-A3-Parent-Top-Tips.pdf |
| **External influences, resources and scares**   * Who is responsible for assessing appropriateness of online resources used in the setting? * What time is given for this? How is this shared with the wider team to promote good practice with parents or good programmes to support learning in the setting? * 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- <https://www.gov.uk/government/publications/challenging-victim-blaming-language-and-behaviours-when-dealing-with-the-online-experiences-of-children-and-young-people> * 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> |

|  |
| --- |
| 2. Policies & PRACTICE |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Policies**   * Do your policies govern all online behaviour, not just when using setting devices or logged into setting systems and platforms? * Do you have an up to date 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 clear if so): * Acceptable Use Policies (AUPs) to reflect varied roles and responsibilities, e.g., parents, staff, visitors, trustees, 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. This should be clear about what social media platforms your setting uses, who has access to this/manages it and what should/should not be published e.g. Do you publish images of children? What measures do you take to protect children if so? * Clear policies for staff taking home tablets, working on learning journeys or nursery documents at home etc. that are linked to the AUPs. * Information sharing protocols - How is confidential information shared with other stakeholders? Are all documents emailed via a secure system? * Do policies state the setting’s expectations regarding professional boundaries/behaviour of staff, including communication via social media and whilst participating in online meetings/training? * Clear policies regarding the expectations for how staff should communicate with parents/carers and colleagues |  |  |  | Several organisations provide customisable templates, including LGfL at <https://safepolicies.lgfl.net>  This guidance from the UK Centre for Internet Safety may be helpful with policy development: <https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-guidance-for-practitioners>  ‘Guidance for safer working practice  for those working with children and young people in education settings’- <https://www.saferrecruitmentconsortium.org/_files/ugd/f576a8_0d079cbe69ea458e9e99fe462e447084.pdf>  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)  Information Commissioners Office (ICO): For information around data protection and GDPR 9 - [www.ico.org.uk/for-organisations/education/](http://www.ico.org.uk/for-organisations/education/) |
| **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 way to tell staff if they have an online safety concern? * Is there any 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).) |
| **Content & review, policy v. practice**   * Do you consult others to populate your policy, e.g. review local templates? * 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 with all stakeholders including team members, parents/carers, committee members and include the voice of the child? * 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 cameras, but photos are required)? * Are new systems, devices, apps, platforms, processes and user behaviour/needs and incidents regularly embedded into these ‘living’ documents? * Are policies updated to reflect children’s needs, behaviour and safeguarding risks and incidents in your setting? |  |  |  |  |

|  |
| --- |
| 3. Training |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Training & CPD**   * Do all staff receive online safety training as part of the safeguarding training schedule? Does this include online safety scenarios to support staff learning? * How does this training reflect the approach you have outlined in this audit and in your policies? * Has the DSL attended any specific training regarding Online Safety (please record the date of this)? * How are ALL staff made aware of and regularly updated on national/regional trends (e.g. Gen AI) and those in the setting relating to general behaviour, harms or incidents? * Is training appropriate to and customised for different roles and responsibilities, with extra strategic elements for room seniors, deputies and committee members? |  |  |  | Look at <https://safetraining.lgfl.net> for access to training offered by LGfL |

[ END OF SECTION 1]

Safe Systems

Settings have a duty to provide safe 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). Settings also need to signpost and support parents with safe systems in the home.

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. Data suggests that many children will start using technology in some form, early in their life and so the education element is key, i.e. teaching children what to do when they see or experience something worrying.

| Question | **F**u**lly In Place** | **Partial/ Needs Review** | **Not In Place** | • Evidence / details and dates  • Any actions / by whom?  *NB – we pre-filled examples / links – delete as appropriate* |
| --- | --- | --- | --- | --- |
| 1. **Technology** | | | | |
| **Controls**   * Have you ensured and checked that safety controls are set on your broadband to restrict inappropriate content? * Have you ensured and checked that safety controls are appropriately in place on every device in the setting? * What are they (separate for each type of device)? * How do you check that these are in place/not disabled? * Who oversees the controls in place? Is this clearly outlined as part of their role and responsibilities? |  |  |  | FREE Policy Guide for Online Safeguarding and Digital Media Use in Early Years Settings – <https://eysafe.lgfl.net>  For advice on this, have a look at: <https://www.internetmatters.org/parental-controls/> |
| **Appropriate filtering**   * Do you use a filtering system in your setting to block inappropriate websites on the internet?   + If so, has your provider filed a submission with the UK Safer Internet Centre to explain why your filtering is ‘appropriate’?   + 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?   + Have DSL, management, administrators and educators all read and understood this submission, including rationale, benefits and limitations and safe search settings, e.g. for web searches and YouTube?   + Do you regularly check your filtering logs to identify any concerns?   + 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)? |  |  |  | Filtering is a system used to block/allow particular websites.  You will find lots of information about filtering here (please note this website is designed specifically for schools) <https://safefiltering.lgfl.net>  Safer Internet Centre submissions for other providers - <https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/filtering-provider-responses>  YouTube guidance - <https://youtube.lgfl.net>  Statement for filtering in general - <https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering>  Filtering logs are the reports generated about what content has been blocked/allowed on your internet.  School based settings and maintained nurseries are required to follow the requirements outlined in [KCSIE](https://assets.publishing.service.gov.uk/media/66d7301b9084b18b95709f75/Keeping_children_safe_in_education_2024.pdf) for filtering, and the [DfE Standards for Filtering and Monitoring](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges) apply to schools. |
| **Monitoring**   * What is your setting’s approach to monitoring/supervising what children do and see when they are using digital technology? * Are children always supervised when using devices? * If staff are always supporting children when devices are used, are staff clear about their role and responsibilities regarding physical monitoring? |  |  |  | The UK Safer Internet Centre provides an overview about what monitoring is: <https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring>  School based settings and maintained nurseries are required to follow the requirements outlined in [KCSIE](https://assets.publishing.service.gov.uk/media/66d7301b9084b18b95709f75/Keeping_children_safe_in_education_2024.pdf) for monitoring, and the [DfE Standards for Filtering and Monitoring](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges) apply to schools.  LGfL have partnered with Senso to offer monitoring: <https://monitoring.lgfl.net> |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Safe modes / search**   * Do you enforce safe search on search engines used (e.g. Google) and block search engines which do not have a safe search? (\*\*enforced means it cannot be turned on and off) * Do you utilise a child friendly search engine if children are using this themselves (and therefore block their access to other search engines)? |  |  |  | Most popular search engines have a Safe Search function which should always be enforced as it will block the most inappropriate of content (e.g. pornography).  Advice on enforcing SafeSearch on a network:   * <https://support.google.com/websearch/answer/186669?hl=en-GB&prev=https://www.google.com/safesearch&dark=1&visit_id=638766100287163031-835895806&p=ws_lock_safesearch&rd=1#zippy=%2Cin-windows> * <https://support.google.com/websearch/answer/510?hl=en-GB&prev=https://www.google.com/safesearch&dark=1&visit_id=638766100287163031-835895806&p=ws_settings_safesearch&rd=1> |
| **YouTube**   * Does pedagogy drive the use of YouTube? i.e. why are children watching videos? What purpose does this serve? * If you use YouTube, which one of the restricted modes do you enforce? * Do you use YouTube Kids to limit inappropriate content (although recognising this is not 100% safe)? * Do you turn the screen off if not required? If you are using YouTube for nursery rhymes and songs, consider turning the screen off and just allowing audio. * YouTube terms and conditions normally allow use by over-13s but require parental permission – how have you sought this and communicated the use of YouTube with parents? * Do you turn off autoplay (to prevent randomised videos playing once the current one is finished) and change the view to cinema mode or full screen (to hide adverts and suggested videos) every time that you open YouTube? * Are all staff aware that adverts before a video may be inappropriate and are in any case not made for children? Do you make every effort to avoid children watching these adverts? * Do you prohibit children from raw scrolling (whereby children scroll on platforms looking for content)? Adults should support children to mindfully choose content, and this content should be checked before children see it to ensure it is safe. * How do you limit children inadvertently seeing inappropriate content? If using sites like YouTube, do you utilise the playlist function? Where possible, when using devices to show things to children, practitioners should be logged in with a professional account and ideally use a playlist rather thanfindingindividual videos as this will limit coming across inappropriate content. Staff avoid giving a device to a child where the adult is logged into their own YouTube account. * Are you mindful about the risks to eye health and posture from using small screens? How do you mitigate this? |  |  |  | YouTube mode checked via <https://youtubemode.lgfl.net>  YouTube settings overview at <https://youtube.lgfl.net>  Turning on restricted mode:  <https://support.google.com/youtube/answer/174084?sjid=8338118240738034422-NC>  Restricting YouTube to users:  <https://support.google.com/a/answer/6214622?hl=en> |
| **Streaming Services**   * Does pedagogy inform why you are streaming videos? i.e. why are children watching videos? What purpose does this serve? * If you allow access to BBC iPlayer, do you have a current TV licence? * Do you have access to Netflix, Disney, Amazon Prime or similar streaming sites? You must not show videos from Netflix, Disney, Amazon Prime or other subscription services as this goes against the terms and conditions. |  |  |  |  |
| **Staff use of devices**   * How do you ensure staff are not accessing their own devices including phones & wearable technology (e.g. smart watches), etc. whilst working with children? * Where do staff keep their personal devices whilst at work? * How do you ensure visitors to the setting are not accessing their own technology, phones, watches, etc. whilst with children? * Are your policies clear about expectations for staff taking imagery of children?   + e.g. on which devices?   + Checking parental consent   + Ensuring images do not humiliate or show children in any state of undress. * What is your approach to checking device settings regularly to ensure imagery and content on these is appropriate? Who does this? How often and where is this recorded? |  |  |  |  |
| **Devices at home**   * How and how often do you remind parents about how to set controls on their home internet/phones/devices etc? * What training/support are you providing to parents/carers on new technology that can support their child’s learning at home? * What guidance are you providing to parents/carers about appropriate time for technology, healthy habits about device use, guidelines for bedtimes, tablets remaining downstairs, etc.? |  |  |  | See <https://parentsafe.lgfl.net> for support with security settings and other ways parents can keep their children safe online |
| 1. cybersecurity | | | | |
| **Audit, policy & documentation** (given its importance for continuity of access to systems and data for keeping children safe, data secure and maintaining continuity of teaching & learning, cybersecurity should be audited separately)   * Does your setting have the 3 documents recommended by 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? |  |  |  | Templates for these three documents including notes to explain to a non-technical audience are at <https://elevate.lgfl.net> |
| **Training**   * Are managers given training and regular reminders on cybersecurity best-practice (passwords, phishing, reporting and more)? * Is this shared with the team and put into practice in office practice and across the setting? |  |  |  | NCSC non-technical training for school staff is available for free, e.g. from LGfL <https://booking.lgfl.net/book/add/p/33> |
| 1. 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 any CCTV or live cameras in your setting, is there a robust policy that ensures you comply with data protection legislation and doesn’t expose children to being seen by people from other families? * Who has access to the recordings from CCTV or other live cameras? How is this managed to safeguard children and protect adults too? |  |  |  | Information Commissioners Office (ICO): information around data protection and GDPR - <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>  Tips for Data Protection in Early Years settings: <https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/data-protection-tips-for-early-years-settings/>  Early Years Alliance guidance on Data Protection: <https://www.eyalliance.org.uk/early-years-settings-and-gdpr>  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) |