LDBS Briefing on changes to Keeping Children Safe in Education 2023

This latest statutory guidance replaces KCSIE 2022. It comes into force on 1 September 2023. [KCSiE 2023](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1161273/Keeping_children_safe_in_education_2023_-_statutory_guidance_for_schools_and_colleges.pdf)

**Implementing the filtering and monitoring standards:**

This is the one real change in KCSiE 23. Please refer to [Meeting the digital and technology standards in schools](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges):

* Schools **should** have implemented the ‘Meeting digital and technology standards in schools and colleges’ guidance;
* Schools **should** meet the Cyber security standards. (Remember the ‘should’ is generally a ‘must’ in KCSIE) see actions below.

Implementing the filtering and monitoring standards:

what you need to do:

**Governing Bodies should support the SLT to ensure that ensure that:**

* effective filtering and monitoring strategies are in place to meet the standard and the risk profile of the school.
* the strategy is reviewed annually *and* when any risk is noted, new technology is introduced or school practice changes.
* school ‘strategy is informed by the filtering and monitoring review’.
* roles and responsibilities are assigned to ensure effective management of the filtering and monitoring systems in school e.g., GB, SLT, DSLs, staff and any IT support provider working with or in school. NB The designated safeguarding lead (DSL) should take lead responsibility for any safeguarding and child protection matters that are picked up through monitoring.  However, for monitoring to be effective, the GB should also ensure that training is provided to make sure that the specialist knowledge of both safeguarding and IT staff is current in relation to filtering and monitoring.
* clear guidance is provided to staff on the types of incidents they may come across e.g., malicious, technical, or of a safeguarding nature, and what to do and who to speak to if they:
* see or suspect unacceptable content has been accessed.
* discover that unacceptable content can be accessed e.g., any failure in the system or misspellings which enable pupils to access unacceptable content.
* discover any abuse of the system.
* come across any restrictions which limit teaching and learning.
* are teaching content which may cause a spike in logs.
* staff provide effective supervision, take steps to maintain awareness of how devices are being used by pupils and report any safeguarding concerns to the DSL.
* filtering blocks harmful and inappropriate content but does not restrict pupils / students from learning how to manage risks (age-appropriate level) or impact negatively on teaching and learning.
* filteringworks on all devices, including mobile devices.
* monitoring enables filtering issues to be picked up and dealt with swiftly, *usually through alerts or observations, allowing prompt action’,*
* the outcome of all filtering issues is recorded.
* the school’s monitoring provision identifies and alerts leaders to behaviours associated with the 4 areas of risk that users may experience when online as noted in the online safety section of [Keeping children safe in education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2).
* school monitoring procedures are reflected in your Acceptable Use Policy and integrated into relevant online safety, safeguarding and organisational policies, such as privacy notices.
* If the school has a technical monitoring system, they will need to conduct their own data protection impact assessment (DPIA) and review the privacy notices of third-party providers. [The DfE data protection toolkit](https://www.gov.uk/guidance/data-protection-in-schools/data-protection-policies-and-procedures) includes guidance on privacy notices and DPIAs, and your Grow DPO can support you in this.
* a technical monitoring system has been applied to the devices, (a school filtering system might not pick up mobile or app content.
* if device monitoring is being managed by IT staff or third-party providers, they should:
* make sure monitoring systems are working as expected.
* provide reporting on pupil device activity.
* receive safeguarding training including online safety.
* record and report safeguarding concerns to the DSL.
* ensure that monitoring data is received in a format that staff can understand.
* ensure that users are identifiable to the school or college, so concerns can be traced back to an individual, including guest accounts.

Cyber security standards:

**Leaders, including Governing Bodies, should ensure that ensure that:**

* all staff have annual cyber security training [Cyber Security training in schools](https://www.ncsc.gov.uk/information/cyber-security-training-schools)
* at least one governor accesses cyber security training- as above.

Other aspects and word changes to note in KCSiE 2023:  
  
**Renting school premises to out of school providers:**

* Schools should check that anyone renting school premises who work with children are meeting the ‘out of school settings’ guidance. (They should have a trained DSL, know specific s/g issues that put children at risk of harm and review performance and suitability of staff / volunteers on a regular basis, all with appropriate training undertaken. [Keeping Children safe during community activities, after school clubs and tuition.](https://www.gov.uk/government/publications/keeping-children-safe-in-out-of-school-settings-code-of-practice/keeping-children-safe-during-community-activities-after-school-clubs-and-tuition-non-statutory-guidance-for-providers-running-out-of-school-settings)
* Allegations related to renting school premises – if schools receive allegations about staff running activities using the premises, they need to follow their own safeguarding policy, which includes contacting the LADO.

Safer Recruitment – “Schools and colleges should inform shortlisted candidates that online searches may be done as part of due diligence checks”.

Legal age for marriage: The age of 18 is now the legal age for marriage- raised in February 2023

Prevent Duty – wording changed from ‘vulnerable’ to children and young people who are ‘susceptible’ to being drawn into terrorism.

Pupils ‘missing in education’ are now ‘absent from education’ – focus remains particularly on pupils absent for prolonged periods or on repeat occasions.

**Other aspects and word changes to note:**

**what you need to do**:  
  
**Leaders, including Governing Bodies, should ensure that ensure that all staff:**

* are aware of the need for companies/clubs using school space for activities outside of school hours to have a DSL and follow the guidance noted above.
* know that if any safeguarding concerns are raised linked to out of school activities on school sites, these should be reported to the DSL.
* know that ‘missing in education’ is now ‘absent from education’.
* know that under the Prevent Duty children are now described as ‘susceptible to being drawn into terrorism’ and no longer ‘vulnerable’ to it.
* know that the age of marriage in the UK is now 18.

Document links:

* LDBS guidance ‘Safeguarding self-evaluation toolkit 23-24’ for detailed support. <https://ldbs.co.uk/policies-downloads/> click on ‘safeguarding’ in drop down menu.
* LDBS overarching shorter checklist which is found at the beginning of the toolkit.
* Keeping Children Safe in Education 2023 [KCSiE 2023](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1161273/Keeping_children_safe_in_education_2023_-_statutory_guidance_for_schools_and_colleges.pdf)
* Keeping Children safe during community activities, after school clubs and tuition. [Keeping Children safe during community activities, after school clubs and tuition.](https://www.gov.uk/government/publications/keeping-children-safe-in-out-of-school-settings-code-of-practice/keeping-children-safe-during-community-activities-after-school-clubs-and-tuition-non-statutory-guidance-for-providers-running-out-of-school-settings)
* Cyber Security training in schools (link above) [Cyber Security training in schools](https://www.ncsc.gov.uk/information/cyber-security-training-schools)
* The filtering and monitoring standards  [https://www.gov.uk/guidance/meeting digital and technology standards in schools and colleges](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges)

##### Your LDBS adviser, Grow Education DPO and Grow safeguarding consultants will be able to support you in aspects noted above.

##### Contact Grow on: **020 7932 1175** / [**grow@london.anglican.org**](mailto:grow@london.anglican.org)

© LDBS 2023

You can copy, download or print this document for use by your school or academy trust as long as you acknowledge the source. You must use the full document; you may not use excerpts or edit it. You may not distribute this document or use it for public or commercial purposes except with our express written permission; all enquiries to [LDBS](mailto:abigail.chand@london.anglican.org).