UK Online Safety Guidance in 2023

A Comprehensive Overview

Introduction

Whilst schools have long been required to do something "appropriate" when it comes to online safety, official guidance on the specifics has always been very weak.[1] However, this year the Department for Education has published brand new *Filtering and Monitoring Standards for Schools and Colleges*. There have also been updates to the UK Safer Internet Centre's *Appropriate Filtering for Education Settings* and *Appropriate Monitoring for Schools*, and to the Department for Education's *Keeping Children Safe in Education* statutory guidance, which came into force on 1st September 2023.

Education is devolved across the UK, with each nation having their own safeguarding and online safety guidance. However, of all the UK nations, the guidance for England is by far the most comprehensive, and if schools in the other nations follow this guidance they will largely be going over and above their own governments' requirements, and be providing a safer environment for the children under their care. There are a few additional requirements placed upon schools outside of England which are noted in the appendix.

This document is split into two main sections: the first aims to provide an overview of what has changed this year, and the second pulls together all of the guidance to provide a comprehensive reference as to what schools are expected to do. Although this is a long document and it is tempting to only read through the updates section, we highly recommend reading the whole document to check whether you are meeting the guidance.

Who are Opendium?

Opendium is a small, specialist UK based, online safety provider who has been supplying UK schools for almost 20 years. We take a very hands-on approach, with the directors frequently spending time on site in order to gain a deep understanding of the issues facing educators when it comes to safeguarding. Our customers include a broad range of schools: primary and secondary state schools, independents, boarding schools and those catering for special educational needs.

Whilst we supply our own filtering and monitoring systems to schools, this document addresses the guidance in general, and should be applicable no matter the system your school uses.

Online safety is a very complex subject, and if you have any questions we are always happy to have a chat. You are welcome to email safeguarding@opendium.com.

1 Some may even say non-existent.

Opendium e-Safety

Table of Contents

What's Changed?

Since last year's update to the Department for Education's *Keeping Children Safe in Education* in September 2022, there have been significant updates to the guidance. These changes were introduced through the June and September 2023 updates to *Keeping Children Safe in Education*,[2] the Department for Education's new *Filtering and Monitoring Standards for Schools and Colleges*,[3] and the latest guidance from the UK Safer Internet Centre.[4]

No updates have been published for the other UK nations, and these updates therefore apply only to England. However, even for schools outside of England, this is still excellent guidance for what constitutes good practice.

Updates to Data Protection

The new information regarding data protection does not change any requirements, it only clarifies what you were already required to do:

- Schools are the data controller of the personal data collected by their filtering (and presumably monitoring) systems.[5] This would usually have been the case previously, but is now specifically mentioned.
- Conduct a Data Protection Impact Assessment (DPIA) regarding the data collected by your filtering and monitoring systems and strategies.[6] It is likely that a DPIA was already required by Article 35 of the the UK GDPR.[7]
- Review the privacy notices of third party providers.[8]
- Ensure you have data sharing or processing agreements with your filtering and monitoring providers.[9] This would have already been required by Article 28 of the UK GDPR. It is worth noting that you need to have data processing or sharing agreements with *any* third parties, such as employers of outsourced ICT staff, who have access to your staff's or students' personal data.[10]

---

2 The Department for Education (England), *Keeping Children Safe in Education*, 2023.
3 The Department for Education (England), *Filtering and Monitoring Standards for Schools and Colleges*, 2023.
4 The UK Safer Internet Centre, *Appropriate Filtering for Education Settings*, 2023;
The UK Safer Internet Centre, *Appropriate Monitoring for Schools*, 2023.
5 *Appropriate Filtering*, "Inappropriate Online Content", ¶ 3.
6 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 8;
Filtering and Monitoring Standards (England), "You should have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 9;
Appropriate Filtering, "Inappropriate Online Content", ¶ 5;
Appropriate Monitoring, ¶ 2.
7 *United Kingdom General Data Protection Regulation*, Article 35.
8 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 8.
9 *Appropriate Filtering*, "Inappropriate Online Content", ¶ 3;
Appropriate Monitoring, ¶ 2.
10 *United Kingdom General Data Protection Regulation*, Article 28.

Updates to Roles and Responsibilities

Who holds the various responsibilities has been clarified, but there is also emphasis on people working together, rather than in isolation, to fulfil these responsibilities.[11]

- Governing bodies and proprietors should identify and assign the roles and responsibilities of staff and third parties (e.g. external service providers).[12] Identify who is responsible for mobile devices, and the filtering and monitoring systems, and ensure that the DSL is also aware.[13]
- There should be a member of the Senior Leadership Team (SLT) and a governor responsible for ensuring that filtering and monitoring standards are met.[14]
- The SLT are responsible for[15]:
    - Documenting decisions on what is blocked or allowed and why.
      Opinion: although the SLT should be involved in setting high level filtering policy, decisions on allowing or blocking specific web sites often need to be made at short notice so it is probably not realistic for the SLT to be directly involved in each decision. Decisions should be documented at the time that they are made, and then reviewed by the SLT on a regular basis. If your filtering system allows you to record notes against allowed / blocked URLs, etc., use that facility as it will help you to understand why a website was whitelisted or blocked when you come to review the system, in the event of an incident, or when you migrate the configuration to a new system were you to change provider in the future.
    - Overseeing reports.
      Opinion: It isn't clear what reports the SLT are expected to oversee. We would expect day to day reports from a monitoring system to go to the DSL. This perhaps refers to the SLT reviewing a regular summary from time to time, which may have been prepared by the DSL for example.
    - Ensuring that staff understand their role, are trained, follow policies, processes and procedures and act on reports and concerns.
- The Designated Safeguarding Lead (DSL) should have an understanding of the filtering and monitoring systems and processes in place.[16]

11 *Filtering and Monitoring Standards (England)*, "You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: The importance of meeting the standard", ¶ 2;
Filtering and Monitoring Standards (England), "You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶¶ 3 - 4.
12 *Filtering and Monitoring Standards (England)*, "You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: How to meet the standard", ¶ 2.
13 *Appropriate Filtering*, ""Filtering on mobile devices";
Appropriate Monitoring, "Monitoring on mobile devices".
14 *Filtering and Monitoring Standards (England)*, "You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: How to meet the standard", ¶ 2.
15 *Filtering and Monitoring Standards (England)*, "You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶¶ 1 - 2.
16 *KCSiE (England)*, ¶ 103.

- The DSL should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:[17]
  - Filtering and monitoring reports.
  - Safeguarding concerns.
  - Checks to filtering and monitoring systems. (See “Checks”, below.)
- The ICT staff have technical responsibility for:[18]
  - Maintaining filtering and monitoring systems.
  - Providing filtering and monitoring reports.
    Opinion: Usually the ICT staff would configure the systems to regularly send suitable automated reports to appropriate staff.
  - Completing actions following concerns or checks to systems.
- If ICT staff or third party providers are managing device monitoring, they will need to record and report safeguarding concerns to the DSL.[19]
- The SLT, DSL and ICT staff should work together to:[20]
  - Procure filtering and monitoring systems. (Primarily the SLT's responsibility.[21])
  - Identify risk.
  - Carry out reviews. (Primarily the SLT's responsibility,[22] and should involve the responsible governor[23]).
  - Carry out checks to filtering and monitoring systems. (See “Checks”, below.)

Updates to Training

- All staff should have an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.[24]

17 *Filtering and Monitoring Standards (England)*, “You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard”, ¶ 5.
18 *Filtering and Monitoring Standards (England)*, “You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard”, ¶ 6.
19 *Filtering and Monitoring Standards (England)*, “You should have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard”, ¶ 3.
20 *Filtering and Monitoring Standards (England)*, “You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard”, ¶ 7.
21 *Filtering and Monitoring Standards (England)*, “You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard”, ¶ 1.
22 *Filtering and Monitoring Standards (England)*, “You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard”, ¶ 1.
23 *Filtering and Monitoring Standards (England)*, “You should review your filtering and monitoring provision at least annually: How to meet the standard”, ¶ 2.
24 *KCSiE (England)*, ¶¶ 14, 124.

- The DSL and ICT staff may need to ask filtering and monitoring providers for system-specific training and support[25].
  Opinion: Far too often, DSLs relay discussions through the ICT staff instead of talking directly to providers.
- If ICT staff are managing device monitoring, they should receive safeguarding training which includes online safety[26].

Updates to Filtering and Monitoring

There is a lot of overlap between filtering and monitoring, so this section covers updates which apply to both, before moving onto separate sections for updates that apply only to one of them.

- Filtering systems and monitoring strategies should be applied to guests, who should be identifiable.[27]
- The requirements for "*age appropriate differentiated filtering*" and "*age appropriate monitoring*", have been extended to be "*context appropriate"* based on age, ability, vulnerability and risk of harm.[28]
- It should not be possible to disable safeguards for illegal content, such as the the Counter-Terrorism Internet Referral Unit (CTIRU) list and child sexual abuse material (CSAM).[29]
  Note that the UK Safer Internet Centre asks for providers to confirm that filtering and monitoring of illegal content cannot be disabled *by the school* whereas their guidance only specifies that the *user* should not be able to disable monitoring of illegal content and that filtering of illegal content simply "*cannot be disabled*" without specifying to whom this applies.
- The list of categories that the filtering system should be able to manage and should be monitored has been extended to include gambling.[30]

25 *Filtering and Monitoring Standards (England)*, "You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶ 4;
Filtering and Monitoring Standards (England), "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: How to meet the standard", ¶ 2.
Filtering and Monitoring Standards (England), "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: How to meet the standard", ¶ 3.

26 *Filtering and Monitoring Standards (England)*, "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard", ¶ 3.

27 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 3;
Filtering and Monitoring Standards (England), "You should have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 4.

28 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 4;
Appropriate Filtering, "Filtering system features", ¶ 1;
Appropriate Monitoring, "Monitoring Strategy/System Features", ¶ 1.

29 *Appropriate Filtering*, "Illegal online content", ¶ 1;
Appropriate Monitoring, "Monitoring content".

30 *Appropriate Filtering*, "Inappropriate Online Content", ¶ 2;
Appropriate Monitoring, "Monitoring content".

- Changes to the monitoring system should be logged "*enabling an audit trail that ensure[s] transparency and that individuals are not able to make unilateral changes*".[31]
- Identify vulnerable users of mobile devices, paying particular attention to ensure that harmful content is not accessible on specific devices.[32]

Updates to Filtering

- You need to understand the coverage of their filtering system, any limitations it has, and mitigate them to minimise harm.[33]
- The filter should be operational and up to date.[34]
- Filtering should be applied to all:[35]
    - Users, including guests.
    - School owned devices (with remote school-owned devices receiving "*the same or equivalent filtering to that provided in school*"[36]).
    - Devices using any of the school's broadband connections (including backup connections).
- The requirement for the system to be able to "*manage relevant languages*"[37] has been clarified to handling "*multilingual web content, images, common misspellings and abbreviations*".[38]
- Filters are now required to block circumvention technologies, such as VPNs,[39] rather than schools just being asked to "consider" how these are handled.[40]
  Opinion: Your filter should be able to block most current VPN technologies. However, these are evolving all the time, with new and clever ways to hide their traffic. Keeping the latest VPN technologies blocked is a game of whack-a-mole, and filtering providers rely on school staff to be vigilant and report to them whenever they spot any students using VPNs.

31 *Appropriate Filtering*, "Filtering system features", ¶ 1;
Appropriate Monitoring, "Monitoring Strategy/System Features", ¶ 1.
32 *Appropriate Filtering*, "Filtering on mobile devices";
Appropriate Monitoring, "Monitoring on mobile devices".
33 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: The importance of meeting the standard", ¶ 2.
34 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 3.
35 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶¶ 3 - 4.
36 *Appropriate Filtering*, "Filtering system features", ¶ 1.
37 *Appropriate Filtering*, "Filtering system features", ¶ 1.
38 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 4.
39 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 4.
40 *Appropriate Filtering*, "Filtering system features", ¶ 1.

- The filtering system should provide alerts when any web content has been blocked.[41] *Opinion: This needs careful consideration to avoid over-alerting. i.e. Use real-time alerts only for things which require immediate intervention such blocked content which could indicate suicidal thoughts or self harm and daily or weekly scheduled reports for less immediate concerns. Consider also that some blocked content may not have been intentionally accessed by a user – for example, your filtering system may routinely block a large amount of incidental content such as adverts from advertisers that are known to show harmful content – is alerting about that blocked content useful?*
- Get confirmation from the filtering provider as to whether they can filter "mobile" or "app" technologies.[42] Previous guidance from the UK Safer Internet Centre said that this should be considered, but the Department for Education's wording is a stronger call to action.
- The requirement for the filtering system to identify individuals[43] (where possible) has now been extended to also identify:[44]
    - Device name or ID.
    - IP address.
    - Time and date of attempted access.
    - The search term or content that was blocked.
- The filtering system should be able to enforce search engines' "Safe Search" mode, or a child friendly search engine.[45]
- Staff should be aware of reporting mechanisms for both safeguarding and technical concerns and report if:[46]
    - they witness or suspect unsuitable material has been accessed;
    - they can access unsuitable material (including where they notice that abbreviations or misspellings allow access to restricted material);
    - they are teaching topics which could create unusual activity on the filtering logs;
    - there is failure in the software or abuse of the system; or

41 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 4.
42 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 5; *Appropriate Filtering*, "Filtering system features", ¶ 1.
43 *Appropriate Filtering*, "Filtering system features", ¶ 1.
44 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 7.
45 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 11; *Appropriate Filtering*, ""Filtering system features", ¶ 1.
46 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 12.

- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks.

- The requirement for the filtering system to analyse the content as it is streamed to the user has been extended to include "*AI generated content.*"[47]
- Whilst schools were already expected to ensure that those managing the filtering system have sufficient capacity and capability, this has now been extended to include any external support providers.[48]
  Opinion: No specific advice is given on how schools can evaluate external companies. We have published our support response and resolution times to support schools in their evaluation.[49]

Updates to Monitoring

- The monitoring strategy should pick up incidents urgently, allowing you to take prompt action and record the outcome.[50]
- Previously, the suggested monitoring strategies were: physical monitoring, live remote supervision and monitoring network traffic, but "*individual device monitoring software*" has now also been added to the list.[51]
- Ensure that monitoring data is in a format that staff can understand.[52]
- Filtering systems may not pick up mobile or app content, so a "*technical monitoring system*" should be applied to those devices.[53]
  Opinion: What is meant by a "technical monitoring system" is not defined. Since the guidance specifically says that one should be used on devices that may not be well filtered by the filtering system, we presume that "technical monitoring system" refers to additional monitoring software installed on the device itself with the ability to automatically identify and send screenshots of concerning activity to appropriate staff.
- The monitoring system should identify and alert to the behaviours associated with each of the 4 risk areas:[54]

47 *Appropriate Filtering*, "Filtering system features", ¶ 1.
48 *Appropriate Filtering*, "Filtering system features", ¶ 2.
49 Opendium, *Appropriate Filtering for Education Settings*, 2023, "Capacity".
50 *Filtering and Monitoring Standards (England)*, "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: The importance of meeting the standard", ¶ 2.
51 *Filtering and Monitoring Standards (England)*, "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: The importance of meeting the standard", ¶ 3;
Appropriate Monitoring, ""Monitoring strategies".
52 *Filtering and Monitoring Standards (England)*, "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard", ¶ 4.
53 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 5.
Filtering and Monitoring Standards (England), "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard", ¶ 5.
54 *Filtering and Monitoring Standards (England)*, "*You should have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard*", ¶ 6;
KCSiE (England), ¶ 136;
The Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.7.

  - Content: illegal / inappropriate / harmful content – porn, fake news, racism, misogyny, self-harm, suicide, anti-semitism.
  - Contact: harmful interaction with other people – peer pressure, advertising, grooming (for sex, crime, financial, etc.)
  - Conduct: risky / harmful online behaviour – exchanging nudes / porn, bullying.
  - Commerce: gambling, inappropriate advertising, phishing, scams.
- Monitoring systems do not remove the need for staff to provide effective supervision and report safeguarding concerns to the DSL, and maintain an awareness of how devices are being used.[55] In particular, these systems are unable to monitor some technologies (e.g. images or videos taken on mobile devices or from cloud storage).[56]
- You should have policies and processes to support those staff responsible for managing monitoring systems.[57]
  Opinion: The notes say that this is to ensure that appropriate action is taken,[58] but it could also be read as providing counselling, etc. to staff who have been exposed to harmful content while reviewing monitoring logs.

Updates to Reviews

- In addition to the existing requirement to carry out an annual review, a review and risk assessment should also be carried out when:[59]
  - A safeguarding risk is identified.
  - Working practices change (e.g. introduction of remote access, BYOD, etc.).
  - New technology is introduced.
  - Any other substantive changes occur.
- The risk assessment should consider the risks that both children and staff may encounter online, together with associated mitigating actions and activities.[60]
- The results of the review should be recorded.[61]

55 *Filtering and Monitoring Standards (England)*, "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard", ¶ 7.
56 *Appropriate Monitoring*, "Monitoring strategies: 3) Physical Monitoring", ¶ 2.
57 *Appropriate Monitoring*, "Monitoring Strategy/System Features", ¶ 2.
58 The UK Safer Internet Centre, *Appropriate Monitoring for Education Settings: Substantive Changes*, 2023.
59 *Filtering and Monitoring Standards (England)*, "You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 4;
Appropriate Filtering, "Risk assessment", ¶ 1;
Appropriate Monitoring, "Risk assessment", ¶ 1.
60 *Appropriate Filtering*, "Risk assessment", ¶ 1;
Appropriate Monitoring, "Risk assessment", ¶ 1.
61 *Filtering and Monitoring Standards (England)*, "You should review your filtering and monitoring provision at least annually: How to meet the standard", ¶ 2;
Filtering and Monitoring Standards (England), "You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 8.

- To carry out the review you need to understand.[62]
  - The risk profile of pupils (ages, special needs / disabilities, whether English is a first or second language).
  - What the filter blocks / allows and why.
  - Any external safeguarding influences (e.g. “county lines” exploitation).
  - Any relevant safeguarding reports.
  - The digital resilience of the pupils.
  - Teaching requirements (e.g. RHSE / PSHE curriculum).
  - The specific use of chosen technologies, including BYOD.
  - The safeguarding / technology policies.
  - What checks are taking place and how resulting actions are handled.
- The review should inform:[63]
  - Safeguarding and technology policies / procedures.
  - Roles and responsibilities.
  - Staff training.
  - Curriculum and learning opportunities.
  - Procurement decisions.
  - What checks are made and how often. (See “Checks”, below.)
  - Monitoring strategies.
- Review and modify blocklists in line with changes to safeguarding risks.[64]
- Audit the mobile device estate, detailing all of the school’s mobile devices, what apps are used and how the apps are installed and deleted. Ensure that apps can be centrally and routinely removed from mobile devices.[65]

62 *Filtering and Monitoring Standards (England)*, “You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard”, ¶ 2;
63 *Filtering and Monitoring Standards (England)*, “You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard”, ¶ 3.
64 *Filtering and Monitoring Standards (England)*, “You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard”, ¶ 9;
65 *Appropriate Filtering*, “Filtering on mobile devices”;
Appropriate Monitoring, “Monitoring on mobile devices”.

Updates to Checks

You are now expected to do regular checks to ensure that your systems are working as expected. Whereas “reviews” refers to regularly reviewing your policies, “checks” is making sure that the systems are still working and configured to support those policies.

Although it would have been good practice to carry out these checks, they were not mentioned by previous guidance. Please see “Checks”, below for details of the checks which should be now carried out.

Other Updates

- Consider meeting the Department for Education’s *Cyber Security Standards for Schools and Colleges*[66].

66 *KCSiE (England)*, ¶ 144;
For more information, refer to: The Department for Education (England), *Cyber Security Standards for Schools and Colleges*, 2023.

Overview of the Current Guidance

This section will concentrate on all of the relevant guidance for England, as it is by far the most comprehensive. Footnotes referencing the equivalent guidance for Wales, Scotland and Northern Ireland are included, and any extra requirements for schools in these nations noted in the appendix.

Opinion: Your approach to online safety is expected to be risk based. There is therefore flexibility, and you should not see the guidance as a rigid set of rules that they must comply with at all costs. However, where you have decided to deviate from the guidance, you should have conducted and documented a thorough risk assessment so that you can show that you have made an informed decision to do so, backed up with strong reasoning and mitigation strategies. Deviation from the guidance should not be done simply for cost savings or to support poor decisions (e.g. poorly chosen equipment, bad network designs, etc.)

Opinion: The UK Safer Internet Centre invites filtering and monitoring system providers to submit responses[67] to their guidance, showing how they comply with it. When making a purchasing decision, and as part of your regular online safety review, it would be wise to use these responses to evaluate suppliers. However, there are a couple of points regarding these documents, that we feel should be considered:

- *It is important to check the date of the response, since the guidance and technologies change from time to time and some suppliers may not have submitted responses to the latest guidance.*
- *Each requirement is open to interpretation and, whilst we wouldn't want to suggest that providers are intentionally trying to mislead, questions will inevitably be interpreted in a way that shows each product in the best light. No provider wants to be the one to say they can't meet a requirement that everyone else is interpreting in a way that allows them to say that they can.*

Data Protection

- Schools are the data controller of the personal data collected by their filtering (and presumably, monitoring) systems.[68]
- Conduct a Data Protection Impact Assessment (DPIA) regarding the data collected by your filtering and monitoring systems and strategies.[69]

67 The UK Safer Internet Centre, *Provider Responses*.
68 *Appropriate Filtering*, "Inappropriate Online Content", ¶ 3.
69 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 8;
Filtering and Monitoring Standards (England), "You should have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 9;
Appropriate Filtering, "Inappropriate Online Content", ¶ 5;
Appropriate Monitoring, ¶ 2.

- Review the privacy notices of third party providers.[70]
- Ensure you have data sharing or processing agreements with your filtering and monitoring providers.[71] It is worth noting that Article 28 of the UK GDPR. requires you to have data processing or sharing agreements with *any* third parties, such as employers of outsourced ICT staff, who have access to your staff's or students' personal data.[72]
- Understand your filtering and monitoring provider's data retention policies.[73]
- Understand what data the monitoring (and presumably, filtering) system stores, and where it is stored (cloud / on-premises) and whether it is backed up.[74]
- Ensure that users understand that their online access is being monitored and that expectations of appropriate use are communicated and agreed.[75] This includes making users who are working remotely aware as to the extent of the monitoring that they receive outside of school.
  Opinion: Filtering and monitoring providers may be able to offer advice, guidance and resources. Although aimed at the providers of online services rather than schools, the Children's Code *from the Information Commissioner's Office contains some relevant guidance, such as ensuring that privacy information is presented in an age appropriate way, which may include using diagrams, cartoons, etc.*[76]

Roles and Responsibilities

The guidance specifies who holds the various responsibilities, but also emphasises that people should working together, rather than in isolation, to fulfil these responsibilities[77].

- Governing bodies and proprietors should identify and assign the roles and responsibilities of staff and third parties (e.g. external service providers).[78] Identify who is responsible for mobile devices, and the filtering and monitoring systems, and ensure that the DSL is also aware.[79]

---

70 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard ", ¶ 8.
71 *Appropriate Filtering*, "Inappropriate Online Content", ¶ 3;
Appropriate Monitoring, ¶ 2.
72 *United Kingdom General Data Protection Regulation*, Article 28.
73 *Appropriate Filtering*, "Inappropriate Online Content" ¶ 3;
Appropriate Monitoring, "Monitoring strategies: 2) Internet and web access"
Appropriate Monitoring, "Monitoring Strategy/System Features", ¶ 1.
74 *Appropriate Monitoring*, "Monitoring Strategy/System Features", ¶ 1.
75 *Appropriate Monitoring*, "Monitoring Strategy/System Features", ¶ 1;
Safeguarding and Child Protection in Schools (NI), § 6.7.
DE Circular 2013/25: eSafety Guidance (NI), ¶¶ 4.2 - 4.3.
76 The Information Commissioner's Office, *Recommended Actions in the Children's Code*, "Privacy information and community standards".
77 *Filtering and Monitoring Standards (England)*, "You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: The importance of meeting the standard", ¶ 2;
Filtering and Monitoring Standards (England), "You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶¶ 3 - 4.
78 *Filtering and Monitoring Standards (England)*, "You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: How to meet the standard", ¶ 2.

- There should be a member of the Senior Leadership Team (SLT) and a governor responsible for ensuring that filtering and monitoring standards are met.[80]
- The SLT are responsible for:[81]
    - Documenting decisions on what is blocked or allowed and why.
      Opinion: although the SLT should be involved in setting high level filtering policy, decisions on allowing or blocking specific web sites often need to be made at short notice so it is probably not realistic for the SLT to be directly involved in each decision. Decisions should be documented at the time that they are made, and then reviewed by the SLT on a regular basis. If your filtering system allows you to record notes against allowed / blocked URLs, etc., use that facility as it will help you to understand why a website was whitelisted or blocked when you come to review the system, in the event of an incident, or when you migrate the configuration to a new system were you to change provider in the future.
    - Overseeing reports.
      Opinion: It isn't clear what reports the SLT are expected to oversee. We would expect day to day reports from a monitoring system to go to the DSL. This perhaps refers to the SLT reviewing a regular summary from time to time, which may have been prepared by the DSL for example.
    - Ensuring that staff understand their role, are trained, follow policies, processes and procedures and act on reports and concerns.
- There should be a Designated Safeguarding Lead (DSL), and they should not be the proprietor of the school.[82]
- The DSL (or a deputy) should always be available during school hours to discuss safeguarding concerns.[83]
- The DSL should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:[84]
    - Filtering and monitoring reports.
    - Safeguarding concerns.
    - Checks to filtering and monitoring systems. (See “Checks”, below.)

79 *Appropriate Filtering*, “Filtering on mobile devices”;
Appropriate Monitoring, “Monitoring on mobile devices”.
80 *Filtering and Monitoring Standards (England)*, “You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: How to meet the standard”, ¶ 2;
Keeping Learners Safe (Wales), ¶ 2.9.
81 *Filtering and Monitoring Standards (England)*, “You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard”, ¶¶ 1 - 2.
82 *KCSiE (England)*, ¶ 103;
Safeguarding and Child Protection in Schools (NI), § 3, 4.1, 4.2.4, 4.2.5, 4.3 and Annex A.
83 *KCSiE (England)*, Annex C.
84 *Filtering and Monitoring Standards (England)*, “You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard”, ¶ 5.

- The ICT staff have technical responsibility for:[85]
  - Maintaining filtering and monitoring systems.
  - Providing filtering and monitoring reports.
    Opinion: Usually the ICT staff would configure the systems to regularly send suitable automated reports to appropriate staff.
  - Completing actions following concerns or checks to systems.
- If ICT staff or third party providers are managing device monitoring, they will need to record and report safeguarding concerns to the DSL.[86]
- The SLT, DSL and ICT staff should work together to:[87]
  - Procure filtering and monitoring systems. (Primarily the SLT's responsibility.[88])
  - Identify risk.
  - Carry out reviews. (Primarily the SLT's responsibility,[89] and should involve the responsible governor[90]).
  - Carry out checks to filtering and monitoring systems. (See “Checks”, below.)

Training

- All staff, governors and trustees should receive safeguarding / child protection / online safety training at induction, including an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.[91]
- Update staff training regularly.[92]
- Staff training should be in line with any advice from safeguarding partners.[93]

85 *Filtering and Monitoring Standards (England)*, “You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard”, ¶ 6.
86 *Filtering and Monitoring Standards (England)*, “You should have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard”, ¶ 3.
87 *Filtering and Monitoring Standards (England)*, “You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard”, ¶ 7.
88 *Filtering and Monitoring Standards (England)*, “You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard”, ¶ 1.
89 *Filtering and Monitoring Standards (England)*, “You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard”, ¶ 1.
90 *Filtering and Monitoring Standards (England)*, “You should review your filtering and monitoring provision at least annually: How to meet the standard”, ¶ 2.
91 *KCSiE (England)*, ¶¶ 14, 124 - 125, Annex A;
Keeping Learners Safe (Wales), ¶¶ 2.5, 2.34, 3.8;
Safeguarding and Child Protection in Schools (NI), § 4.1;
The Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, ¶ 4.1.i.
92 *KCSiE (England)*, ¶¶ 14, 124 - 125, Annex A;
Keeping Learners Safe (Wales), ¶¶ 2.36, 3.8;
Safeguarding and Child Protection in Schools (NI), § 4.1.
93 *KCSiE (England)*, ¶¶ 14, 124 - 125, Annex A.

- The training should be "*integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning*".[94]
- Send regular safeguarding / child protection / online safety updates to all staff (via email, e-bulletins, staff meetings, etc.) as required, at least annually.[95]
- Staff should have an awareness that technology is a significant component in many safeguarding / well being issues.[96]
- Separate training may be needed for governors and trustees, since they are involved in setting and testing safeguarding policies.[97]
- The SLT and relevant staff should have an awareness and understanding of the provisions in place, how to manage them effectively and how to escalate concerns.[98]
- Train and refresh the knowledge and skills of the DSL and deputies at regular intervals and at least annually, such that they.[99]
    - "*are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school or college*"; and
    - "*can recognise the additional risks that children with special educational needs and disabilities (SEND) face online, for example, from bullying, grooming and radicalisation and are confident they have the capability to support children with SEND to stay safe online.*"
- The DSL and ICT staff may need to ask filtering and monitoring providers for system-specific training and support[100].
  Opinion: Far too often, DSLs relay discussions through the ICT staff instead of talking directly to providers.
- If ICT staff are managing device monitoring, they should receive safeguarding training which includes online safety[101].

94 KCSiE (England), ¶ 127.
95 KCSiE (England), ¶¶ 14, 124 - 125, Annex A;
Keeping Learners Safe (Wales), ¶ 3.6.
96 KCSiE (England), ¶¶ 24, 32, 35, 156, Annex A.
97 KCSiE (England), ¶ 81;
Keeping Learners Safe (Wales), ¶¶ 2.5, 2.11.
98 KCSiE (England), ¶ 141.
99 KCSiE (England), Annex C;
Safeguarding and Child Protection in Schools (NI), § 4.7.2.
100 Filtering and Monitoring Standards (England), "You should identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶ 4;
Filtering and Monitoring Standards (England), "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: How to meet the standard", ¶ 2.
Filtering and Monitoring Standards (England), "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: How to meet the standard", ¶ 3.
101 Filtering and Monitoring Standards (England), "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard", ¶ 3.

Teaching

- Teach the children about how to keep themselves and others safe, including online. The education should be tailored to individual children's needs (taking into account abuse victims, SEN, disabilities).[102] *Keeping Children Safe in Education* links to various resources for teaching online safety. This also makes up part of Ofsted's and Estyn's inspection frameworks.[103]

Filtering and Monitoring

There is a lot of overlap between filtering and monitoring, so this section covers guidance which applies to both, before moving onto separate sections for guidance that applies only to one of them.

- You should have "appropriate" filtering systems and monitoring strategies to limit children's exposure to risks.[104]
- The Department for Education's *Schools' Buying Strategy* and *Buying for Schools* advice is signposted.[105] The main advice in these is for schools to either purchase through a framework agreement, or get quotes from at least 3 suppliers, and to consider what after-sales support you will get.
  Opinion: The latter point is important and often overlooked. Although it is important to manage the budget, many of our customers have come to us not for the cost savings, but because they felt that their existing provider was not providing a high enough level of support.
- Carry out a risk assessment and use it to inform filtering and monitoring provision.[106]

102 *KCSiE (England)*, ¶¶ 129, 133.
The Welsh Government, *Education Digital Standards for Schools in Wales: Web filtering*, 2021, ¶¶ 4 -5;
Safeguarding and Child Protection in Schools (NI), § 6.7;
The Department of Education (Northern Ireland), *DE Circular 2016/27: Online Safety*, ¶¶ 9, 17;
The Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, ¶ 2.5;
The Department of Education (Northern Ireland), *DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools*, ¶ 2;
The Department of Education (Northern Ireland), *Education in Safe and Effective Practices*;
Appropriate Filtering, "Filtering system features" ¶ 3;
Appropriate Monitoring, "Monitoring Strategy/System Features", ¶ 3.

103 Ofsted, *School Inspection Handbook*, 2022, ¶ 293;
Estyn, *Guidance for Inspectors*, 2022, § 3.1.

104 *KCSiE (England)*, ¶¶ 138, 141;
Keeping Learners Safe (Wales), ¶ 7.7.
The Scottish Government, *Internet Safety for Children and Young People: National Action Plan*, 2017, "Every child and young person has an age appropriate and evolving understanding of the opportunities and risks which exist in in the online world: Prevent Activity";
Safeguarding and Child Protection in Schools (NI), § 6.8;
DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools (NI) ¶ 2.ii;
DE Circular 2013/25: eSafety Guidance (NI), ¶ 4.2.

105 *KCSiE (England)*, ¶ 143;
For more information, refer to: The Department for Education (England), *Schools' Buying Strategy*, 2021 and The Department for Education (England), *Buying for Schools*, 2023.

106 *KCSiE (England)*, ¶ 142;
Appropriate Filtering, "Risk assessment" ¶ 1;
Appropriate Monitoring, "Risk assessment", ¶ 1;
Safeguarding and Child Protection in Schools (NI), § 6.8;

- Filtering systems and monitoring strategies should also be applied to guests, who should be identifiable.[107]
- Filtering and monitoring should handle multilingual web content, images, common misspellings and abbreviations.[108]
- Filtering and monitoring should be "*context appropriate"* based on age, ability, vulnerability and risk of harm.[109]
- It should not be possible to disable safeguards for illegal content, such as the the Counter-Terrorism Internet Referral Unit (CTIRU) list and child sexual abuse material (CSAM).[110] Note that the UK Safer Internet Centre asks for providers to confirm that filtering and monitoring of illegal content cannot be disabled *by the school* whereas their guidance only specifies that the *user* should not be able to disable monitoring of illegal content and that filtering of illegal content simply "*cannot be disabled*" without specifying to whom this applies.
- You should be able to control filtering and monitoring systems themselves in order to permit or deny access to specific content,[111] and be able to change the keywords which the monitoring system uses to trigger alerts.[112]
  Opinion: It is important for you to be able to control their own systems so that you can implement configuration changes quickly when problems occur, to avoid impacting teaching. However, it is very easy to inadvertently turn off filtering to large swathes of the internet, and for this reason it is equally important to have easy access to support from the filtering provider. For example, we have seen numerous examples where even educational software vendors have supplied "firewalling instructions" which tell schools that, in order to use a piece of software, they must whitelist huge services such as Amazon Web Services (AWS), or Cloudflare. You might blindly follow those instructions and endanger their children, whereas the filtering provider would easily spot a problem and be able to help put together a safer configuration.

DE Circular 2013/25: eSafety Guidance (NI), ¶ 4.1.iii.

107 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 3;
Filtering and Monitoring Standards (England), "You should have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 4.

108 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 4;
Appropriate Filtering, ""Filtering system features", ¶ 1.
Appropriate Monitoring, "Monitoring Strategy/System Features", ¶ 1.

109 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 4;
Appropriate Filtering, "Filtering system features", ¶ 1;
Appropriate Monitoring, "Monitoring Strategy/System Features", ¶ 1.

110 *Appropriate Filtering*, "Illegal online content", ¶ 1;
Appropriate Monitoring, "Monitoring content".

111 *Appropriate Filtering*, "Filtering system features" ¶ 1;
Appropriate Monitoring, "Monitoring Strategy/System Features", ¶ 1.

112 *Appropriate Monitoring*, "Monitoring Strategy/System Features", ¶ 1.

- Changes to the filtering and monitoring systems should be logged "*enabling an audit trail that ensure[s] transparency and that individuals are not able to make unilateral changes*".[113]
- The filtering system and monitoring strategy should be able to manage the following categories of content at a minimum:[114]

Category	Filtering	Monitoring
Illegal content (child abuse images and terrorist content)	✓	✓
Bullying		✓
Child sexual exploitation		✓
Discrimination	✓	✓
Drugs / substance abuse	✓	✓
Extremism	✓	✓
Gambling	✓	✓
Malware / hacking	✓	
Pornography	✓	✓
Piracy and copyright theft	✓	
Self harm	✓	✓
Suicide	✓	✓
Violence	✓	✓

Note: blocking and monitoring illegal content is mandatory.[115]

- You should recognise that no filtering or monitoring system is 100% effective and needs to be supported by good teaching, effective supervision, and for staff to report safeguarding concerns to the DSL and maintain an awareness of how devices are being used.[116] In particular, some technologies cannot be monitored using other strategies (e.g. images or videos taken on mobile devices or from cloud storage).[117]

113 *Appropriate Filtering*, "Filtering system features", ¶ 1;
Appropriate Monitoring, "Monitoring Strategy/System Features", ¶ 1.
114 *Appropriate Filtering*, "Inappropriate Online Content" ¶ 1;
Appropriate Monitoring, "Monitoring content".
115 *Filtering and Monitoring Standards (England)*, "You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 1;
Appropriate Filtering, "Illegal online content";
Appropriate Monitoring, "Monitoring content".
116 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: The importance of meeting the standard", ¶ 2;
Filtering and Monitoring Standards (England), "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard", ¶ 7;
Appropriate Filtering, ¶ 6;
Appropriate Monitoring, "Monitoring strategies: 3) Physical Monitoring", ¶ 2;
Appropriate Monitoring, "Monitoring content";
The Department of Education (Northern Ireland), *DE Circular 2011/22: Internet Safety* ¶ 4.
117 *Appropriate Monitoring*, "Monitoring strategies: 3) Physical Monitoring", ¶ 2.

- You should have the ability to deploy a central policy to multiple schools, and to have a centralised dashboard providing oversight.[118]
  Opinion: Whether this is important functionality depends upon whether you are a member of a group, such as a Multi Academy Trust (MAT), and how the MAT is organised. This is clearly an advantage to MATs that want to manage the online safety policies and safeguarding responsibilities of their schools more centrally, whereas in other circumstances these responsibilities may be delegated to the individual schools.

- Ensure that there is sufficient capacity and capability in those responsible for, and those managing, the filtering system and monitoring strategy (**including external support providers**).[119]
  Opinion: No specific advice is given on how schools can evaluate external companies. We have published our support response and resolution times to support schools in their evaluation.[120]

- Identify vulnerable users of mobile devices, paying particular attention to ensure that harmful content is not accessible on specific devices.[121]

Filtering

- Ensure that harmful and inappropriate content is blocked.[122] However, the filter should not "over-block", which would unreasonably affect teaching, learning or school administration, and restrict students from learning how to assess and manage risk themselves[123].
  Boarding schools also have the additional requirement that "*appropriate internet access, is provided for boarders for the purposes of organised and private study outside school hours and **for social purposes**.*"[124] Boarding schools may therefore have to provide access to social networks. This, and the requirement to teach online safety, is backed up by Ofsted's report on *The Safe Use of New Technologies* which found that "*Pupils in the schools that had 'managed' systems had better knowledge and understanding of how to stay safe than those in schools with 'locked down' systems. Pupils were more vulnerable overall when schools used locked down systems because they were not given enough opportunities to learn how to assess and manage risk for themselves*".[125] One of the recommendations to come out of the report was that schools should "*manage the transition from locked down*

118 *Appropriate Filtering*, "Filtering system features" ¶ 1;
Appropriate Monitoring, "Monitoring Strategy/System Features", ¶ 1.
119 *Appropriate Filtering*, "Filtering system features", ¶ 2;
Appropriate Monitoring, "Monitoring Strategy/System Features", ¶ 2.
120 Opendium, *Appropriate Filtering for Education Settings*, 2023, "Capacity".
121 *Appropriate Filtering*, "Filtering on mobile devices";
Appropriate Monitoring, "Monitoring on mobile devices".
122 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: The importance of meeting the standard", ¶ 3;
Safeguarding and Child Protection in Schools (NI), § 6.8.
123 *KCSiE (England)*, ¶ 134.
Filtering and Monitoring Standards (England), "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: The importance of meeting the standard", ¶ 3;
DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools (NI), ¶ 2.
124 The Department for Education (England), *National Minimum Standards for Boarding Schools*, 2022, ¶ 4.2.
125 Ofsted, *The Safe Use of New Technologies*, 2010, p 5.

systems to more managed systems to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school."[126]

- You need to understand the coverage of your filtering system, any limitations it has, and mitigate them to minimise harm.[127]
- The filtering provider should be an IWF member.[128]
- The filter should be operational and up to date.[129]
- Filtering should be applied to all:[130]
  - Users, including guests.
  - School owned devices (with remote school-owned devices receiving "*the same or equivalent filtering to that provided in school*"[131]).
  - Devices using any of the school's broadband connections (including backup connections).
- Circumvention attempts (e.g. VPNs, proxies) should be identified and blocked.[132]
  Opinion: Your filter should be able to block most current VPN technologies. However, these are evolving all the time, with new and clever ways to hide their traffic. Keeping the latest VPN technologies blocked is a game of whack-a-mole, and filtering providers rely on school staff to be vigilant and report to them whenever they spot any students using VPNs.
- The filtering system should provide alerts when any web content has been blocked.[133]
  Opinion: This needs careful consideration to avoid over-alerting. i.e. Use real-time alerts only for things which require immediate intervention such blocked content which could indicate suicidal thoughts or self harm and daily or weekly scheduled reports for less immediate concerns. Consider also that some blocked content may not have been intentionally accessed by a user – for example, your filtering system may routinely block a large amount of incidental content such as adverts from advertisers that are known to show harmful content – is alerting about that blocked content useful?

126 *The Safe Use of New Technologies*, p 6.
127 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: The importance of meeting the standard", ¶ 2.
128 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 1; *Appropriate Filtering*, "Illegal online content".
129 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 3.
130 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶¶ 3 - 4.
131 *Appropriate Filtering*, "Filtering system features", ¶ 1.
132 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 4; *Appropriate Filtering*, "Filtering system features", ¶ 1.
133 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 4.

- Get confirmation from the filtering provider as to whether they can filter “mobile” or “app” technologies.[134]
- The filtering system should allow you to identify[135]:
  - Device name or ID.
  - The individual.
  - IP address.
  - Time and date of attempted access.
  - The search term or content that was blocked.
- The filtering system should be able to enforce search engines' “Safe Search” mode, or a child friendly search engine.[136]
- Staff should be aware of reporting mechanisms for both safeguarding and technical concerns and report if:[137]
  - they witness or suspect unsuitable material has been accessed;
  - they can access unsuitable material (including where they notice that abbreviations or misspellings allow access to restricted material);
  - they are teaching topics which could create unusual activity on the filtering logs;
  - there is failure in the software or abuse of the system; or
  - there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks.
- The filtering system should analyse content (including that delivered over encrypted HTTPS) as it is streamed to the user and block it, taking context into account.[138]
- The filtering provider should publish a rationale that details their approach to filtering and over-blocking.[139]

134 *Filtering and Monitoring Standards (England)*, “Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard”, ¶ 5; *Appropriate Filtering*, “Filtering system features”, ¶ 1.
135 *Filtering and Monitoring Standards (England)*, “Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard”, ¶ 7; *Appropriate Filtering*, “Filtering system features” ¶ 1.
136 *Filtering and Monitoring Standards (England)*, “Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard”, ¶ 11; *Appropriate Filtering*, “Filtering system features”, ¶ 1.
137 *Filtering and Monitoring Standards (England)*, “Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard”, ¶ 12.
138 *Appropriate Filtering*, “Filtering system features” ¶ 1.
139 *Appropriate Filtering*, “Filtering system features” ¶ 1.

- Within the school, filtering should be applied at the network level rather than being reliant upon any software installed on user devices.[140] (However, it is accepted that filtering devices outside of the school may require such software to be installed.)
- There should be a way for users to report content which has been either over-blocked or under-blocked.[141]
- The filtering system should provide clear information on users' historical web browsing activity.[142]

Monitoring

- You do not necessarily need a technological monitoring *system* (although even the most rudimentary filtering system would usually provide some monitoring capabilities). The guidance instead refers to monitoring *strategies*, with these possible strategies listed:[143]
  - Physical monitoring by staff watching the users.
  - Live remote supervision by staff.
  - Network traffic monitoring.
  - Individual device monitoring software / services.
- The monitoring strategy should pick up incidents urgently, allowing you to take prompt action and record the outcome.[144]
- Ensure that monitoring data is in a format that staff can understand, is regularly reviewed and alerts prioritised.[145] How are alerts recorded, communicated and escalated?[146]
- The monitoring strategy should be able to identify users, including guests.[147]
- Filtering systems may not pick up mobile or app content, so a "*technical monitoring system*" should be applied to those devices.[148]
  Opinion: What is meant by a "technical monitoring system" is not defined. Since the

140 *Appropriate Filtering*, "Filtering system features" ¶ 1.
141 *Appropriate Filtering*, "Filtering system features" ¶ 1.
142 *Appropriate Filtering*, "Filtering system features" ¶ 1.
143 *Filtering and Monitoring Standards (England)*, "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: The importance of meeting the standard", ¶ 3;
Appropriate Monitoring, "Monitoring strategies", ¶ .
144 *Filtering and Monitoring Standards (England)*, "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: The importance of meeting the standard", ¶ 2.
145 *Filtering and Monitoring Standards (England)*, "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard", ¶ 4;
Appropriate Monitoring, "Monitoring strategies: 2) Internet and web access";
Appropriate Monitoring, "Monitoring Strategy/System Features", ¶ 1.
146 *Appropriate Monitoring*, "Monitoring Strategy/System Features", ¶ 1.
147 *Filtering and Monitoring Standards (England)*, "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard", ¶ 4;
Appropriate Monitoring, "Monitoring strategies: 2) Internet and web access".
148 *Filtering and Monitoring Standards (England)*, "Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 5.
Filtering and Monitoring Standards (England), "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard", ¶ 5.

guidance specifically says that one should be used on devices that may not be well filtered by the filtering system, we presume that "technical monitoring system" refers to additional monitoring software installed on the device itself with the ability to automatically identify and send screenshots of concerning activity to appropriate staff.

- The monitoring system should identify and alert to the behaviours associated with each[149] of the 4 risk areas:[150]
  - Content: illegal / inappropriate / harmful content – porn, fake news, racism, misogyny, self-harm, suicide, anti-semitism.
  - Contact: harmful interaction with other people – peer pressure, advertising, grooming (for sex, crime, financial, etc.)
  - Conduct: risky / harmful online behaviour – exchanging nudes / porn, bullying.
  - Commerce: gambling, inappropriate advertising, phishing, scams.
- You should be aware of any limitations of the logfile information produced by your filtering and monitoring systems.[151]
- Pro-active monitoring systems are available, whereby alerts are managed and supported by a third-party provider.[152] This relieves you of some of the work and ensures that genuine threats to health and life are escalated. Ensure that the provider's SLA meets your requirements.
- If you operate a BYOD (Bring Your Own Device) system, consider whether you are able to monitor personal devices and mobile apps and ensure accordance with policy and data protection.[153]
- If the monitoring system requires software to be installed on devices, understand what types of device or operating systems it supports and whether this meets your requirements.[154]
- Consider whether personal devices (i.e. not owned by the school) are monitored beyond the school hours and location.[155]
  Opinion: Whilst monitoring personal devices outside of school may yield data which could help with safeguarding, many schools, parents and children would consider this to be outside of the school's remit unless it were offered to parents as an additional ***optional*** *service.*

149 *Filtering and Monitoring Standards (England)*, "You should have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard", ¶ 6.
150 *KCSiE (England)*, ¶ 136.
Safeguarding and Child Protection in Schools (NI), § 6.7.
151 *Appropriate Monitoring*, "Monitoring strategies: 2) Internet and web access".
152 *Appropriate Monitoring*, "Monitoring strategies: 3) Active/Pro-active technology monitoring services".
153 *Appropriate Monitoring*, "Monitoring Strategy/System Features", ¶ 1.
154 *Appropriate Monitoring*, "Monitoring Strategy/System Features", ¶ 1.
155 *Appropriate Monitoring*, "Monitoring Strategy/System Features", ¶ 1.

- The monitoring system should detect harmful images. For example, using image hashes is one strategy, but different providers approach this in different ways.[156]
- Where users are working remotely, understand the extent to which they are monitored while outside of the school premises.[157]
- You should have policies and processes to support those staff responsible for managing monitoring systems.[158]
  Opinion: The notes say that this is to ensure that appropriate action is taken,[159] but it could also be read as providing counselling, etc. to staff who have been exposed to harmful content while reviewing monitoring logs.

Reviews

- Regularly review the effectiveness of the filtering and monitoring systems,[160] and carry out an annual review of the school's approach to online safety, including redoing risk assessments.[161] The 360 Safe website and LGfL online safety audit are both signposted.[162]
- The review and risk assessment should be carried out.[163]
  - At least annually.
  - When a safeguarding risk is identified.
  - When working practices change (e.g. introduction of remote access, BYOD, etc.).
  - When new technology is introduced.
  - When any other substantive changes occur.
- The risk assessment should consider the risks that both children and staff may encounter online, together with associated mitigating actions and activities.[164]

156 *Appropriate Monitoring*, "Monitoring Strategy/System Features", ¶ 1.
157 *Appropriate Monitoring*, "Monitoring Strategy/System Features", ¶ 1.
158 *Appropriate Monitoring*, "Monitoring Strategy/System Features", ¶ 2.
159 *Appropriate Monitoring for Education Settings: Substantive Changes*.
160 *KCSiE (England)*, ¶ 141;
Keeping Learners Safe (Wales), ¶¶ 1.44, 2.9, 2.25, 7.4;
DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools (NI), ¶ 1.
161 *KCSiE (England)*, ¶ 145;
Safeguarding and Child Protection in Schools (NI), §§ 4.1 - 4.2, 4.3.1, 6.8, 6.9.2;
DE Circular 2013/25: eSafety Guidance (NI), ¶ 4.1.iii;
Appropriate Filtering, "Risk assessment";
Appropriate Monitoring, "Risk assessment".
162 For more information, refer to: https://360safe.org.uk/ and https://onlinesafetyaudit.lgfl.net/.
163 *Filtering and Monitoring Standards (England)*, "You should review your filtering and monitoring provision at least annually: The importance of meeting the standard", ¶ 2;
Filtering and Monitoring Standards (England), "You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 4;
Appropriate Filtering, "Risk assessment", ¶ 1;
Appropriate Monitoring, "Risk assessment", ¶ 1.
164 *Appropriate Filtering*, "Risk assessment", ¶ 1;
Appropriate Monitoring, "Risk assessment", ¶ 1.

- The results of the review should be recorded.[165]
- To carry out the review you need to understand.[166]
    - The risk profile of pupils (ages, special needs / disabilities, whether English is a first or second language).
    - What the filter blocks / allows and why.
    - Any external safeguarding influences (e.g. “county lines” exploitation).
    - Any relevant safeguarding reports.
    - The digital resilience of the pupils.
    - Teaching requirements (e.g. RHSE / PSHE curriculum).
    - The specific use of chosen technologies, including BYOD.
    - The safeguarding / technology policies.
    - What checks are taking place and how resulting actions are handled.
- The review should inform:[167]
    - Safeguarding and technology policies / procedures.
    - Roles and responsibilities.
    - Staff training.
    - Curriculum and learning opportunities.
    - Procurement decisions.
    - What checks are made and how often. (See “Checks”, below.)
    - Monitoring strategies.
- Review and modify blocklists in line with changes to safeguarding risks.[168]
- Audit the mobile device estate, detailing all of the school’s mobile devices, what apps are used and how the apps are installed and deleted. Ensure that apps can be centrally and routinely removed from mobile devices.[169]

---

165 *Filtering and Monitoring Standards (England)*, “You should review your filtering and monitoring provision at least annually: How to meet the standard”, ¶ 2;
Filtering and Monitoring Standards (England), “You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard”, ¶ 8.

166 *Filtering and Monitoring Standards (England)*, “You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard”, ¶ 2;

167 *Filtering and Monitoring Standards (England)*, “You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard”, ¶ 3.

168 *Filtering and Monitoring Standards (England)*, “You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard”, ¶ 9.

169 *Appropriate Filtering*, “Filtering on mobile devices”;
Appropriate Monitoring, “Monitoring on mobile devices”.

- Review security protection procedures periodically to keep up with evolving cyber-crime technologies.[170]
- Consider how monitoring reports inform your policy and practice?[171]

Checks

Whereas regular "reviews" are needed to ensure that policies and processes are remaining current, you also need to perform regular "checks" to ensure that filtering and monitoring provision has not been deactivated and is configured and working in line with those policies.[172]

- Checks should include a range of:[173]
  - School owned devices and services, including those used off site.
  - Geographical areas across the site, and off-site (where appropriate).
  - User groups, for example, teachers, pupils and guests.
  - Installed mobile apps (not just internet browsers).
- Carry out checks:
  - On new devices before they are released to staff or pupils.[174]
  - When significant changes have taken place(including policy and legislative changes).[175]
- Document the date and time when each check was done, who did the check, what they checked and what the resulting actions were.[176]
- The SWGfL's testfiltering.com tool is signposted.[177]
  Opinion: although this is a good place to start, this tool only performs a few rudimentary

170 *KCSiE (England)*, ¶ 144.
171 *Appropriate Monitoring*, "Monitoring Strategy/System Features", ¶ 1.
172 *Filtering and Monitoring Standards (England)*, "You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶¶ 6 - 7;
Appropriate Filtering, "Checks and documentation" ¶ 1;
Appropriate Monitoring, "Checks and documentation".
173 *Filtering and Monitoring Standards (England)*, "You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 7;
Appropriate Filtering, "Filtering on mobile devices";
Appropriate Monitoring, "Checks and documentation".
174 *Filtering and Monitoring Standards (England)*, "You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 9.
175 *Appropriate Filtering*, "Checks and documentation" ¶ 1;
Appropriate Monitoring, "Checks and documentation".
176 *Filtering and Monitoring Standards (England)*, "You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 8;
Appropriate Filtering, "Checks and documentation" ¶ 1;
Appropriate Monitoring, "Checks and documentation"
177 *KCSiE (England)*, ¶ 142;
Filtering and Monitoring Standards (England), "You should review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 10;
Appropriate Filtering, "Checks and documentation" ¶ 2;
Appropriate Filtering, "Filtering on mobile devices";
Appropriate Monitoring, "Monitoring on mobile devices".

checks. You may want to do some more robust checks, such as confirming that encrypted HTTPS content is filtered and monitored as expected and that the appropriate categories are filtered and monitored.

Other

- You should have a "whole school" approach to online safety, with mechanisms to identify, intervene and escalate concerns.[178]
- Try to engage with parents when setting online safety policies and what systems the schools are using for filtering and monitoring.[179]
- Have a clear policy on the use of mobile and smart technology, reflecting the fact that many children have unrestricted mobile internet access which will not be filtered / monitored by the school network.[180]
  Opinion: The guidance is particularly weak on the subject of personal mobile devices and mobile data, only saying that you "should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy." With appropriate network level monitoring and filtering, children using your network are inherently safer than those using personal data, even though there are some apps that cannot be monitored. Inviting them to connect personal devices to a relatively permissive wifi network may well be a reasonable approach.
- Several links are provided to information about safeguarding when offering remote learning.[181] These make points such as:
  - Communicate with parents to suggest turning on their ISP's filters.
  - Use approved channels and school accounts for communications.
- Ensure there's an appropriate level of security protection procedures in place to safeguard systems, staff and learners and consider meeting the Department for Education's *Cyber Security Standards for Schools and Colleges*.[182] This refers to security rather than safety – e.g. virus scanners, firewalls, etc.
- Treat sexual abuse that occurs online or outside school equally seriously as abuse that occurs on school premises.[183]

178 *KCSiE (England)*, ¶¶ 135, 137;
Safeguarding and Child Protection in Schools (NI), § 6.7;
DE Circular 2016/27: Online Safety (NI), ¶ 9.
179 *KCSiE (England)*, ¶¶ 137, 140.
180 *KCSiE (England)*, ¶ 138;
DE Circular 2013/25: eSafety Guidance (NI), ¶ 5.3;
National Minimum Standards for Boarding Schools (England), ¶ 8.4.
181 *KCSiE (England)*, ¶ 139;
Safeguarding and Child Protection in Schools (NI), § 6.8, Annex C.
182 *KCSiE (England)*, ¶ 144;
DE Circular 2013/25: eSafety Guidance (NI), ¶ 4.2.
For more information, refer to: The Department for Education (England), *Cyber Security Standards for Schools and Colleges*, 2023.
183 *KCSiE (England)*, ¶¶ 469, 483.

A Final Word

Never before have British schools had such comprehensive guidance as to their responsibilities with regards to online safety. A lot of the new guidance refers to things that many schools would have already been doing as a matter of good practice, but there are certainly key areas in the guidance where a large number of schools will to have to do work to change policies and replace technology. In some cases schools may well find that there is a significant amount of work involved.

One of the main points raised by the updated guidance is that online safety is a cross-discipline job and that no one should be working in isolation. Not only should staff within the school work together to meet these objectives, but they should involve their filtering and monitoring providers, who have many years of experience and can provide insight not only into the capabilities of their products, but also as to how other schools have met the challenges that you face.

If you have any questions, we are always happy to have a chat and you are welcome to email safeguarding@opendium.com.

> "*Schools need an online safety provider they can rely on. Opendium's depth of knowledge and dedication is second to none.*"
>
> — Robert Kanaka, ICT Infrastructure Manager, Sherborne Group.

> "*I would highly recommend Opendium to anyone looking for either a filtering solution, or network support specialists. They really are a great team to work with.*"
>
> — Mr O J Rokson, Assistant Head (Digital Strategy), King Edward VI School.

Appendix - The Devolved Administrations

None of the guidance from the devolved administrations is as comprehensive as the English guidance and schools who follow the ""Overview of the Current Guidance" above will therefore be going above and beyond their obligations. However, there are some key differences which should be noted.

Wales

Roles

- Whereas in England schools have a Designated Safeguarding Lead (DSL) (and deputies), in Wales these are known as Designated Safeguarding Persons (DSPs), one of which should be identified as having lead responsibility.[184]
- DSPs should be members of the SLT (but should have deputies, who aren't required to be SLT members), and there is no prohibition on the proprietor of the school being a DSP.[185]
- In England, there should be a governor responsible for ensuring that filtering and monitoring standards are met, but in Wales this role is broader such that there should be a Designated Governor for Safeguarding.[186]

Training

- The staff training requirements are largely the same as in England, but the guidance doesn't refer to *online* safety specifically and instead just refers to safeguarding in general. However, the Welsh guidance does specifically mention that the DSP should have online safety training.[187]
- The DSP should provide an annual briefing and regular updates at staff meetings.[188]

Filtering

- The guidance refers to the *Education Digital Standards for Schools in Wales* "*Web filtering*" document,[189] instead of the UK Safer Internet Centre's guidance. This document contains an exhaustive list of categories and specifies whether they are to be allowed or blocked at each key stage, and in that respect it is a lot more informative and rigid than the English guidance. However, the UK Safer Internet Centre's guidance addresses much broader and more nuanced aspects of filtering but is not signposted at all by the Welsh guidance. Also note that each filtering provider has their own set of categories, and as the "Web filtering"

184 *Keeping Learners Safe (Wales)*, ¶¶ 2.14 - 2.15.
185 *Keeping Learners Safe (Wales)*, ¶ 2.16.
186 *Keeping Learners Safe (Wales)*, ¶ 2.9.
187 *Keeping Learners Safe (Wales)*, ¶ 2.14.
188 *Keeping Learners Safe (Wales)*, ¶ 3.60.
189 *Keeping Learners Safe (Wales)*, ¶ 7.7;
For more information, refer to: Education Digital Standards for Schools in Wales: Web filtering.

document was developed in collaboration with Smoothwall the categories it lists are Smoothwall's. Mapping this exhaustive list of categories onto another product is not straight forward.

Monitoring

- Welsh schools are also required to have "appropriate" monitoring,[190] but no guidance, such as the UK Safer Internet Centre's, is signposted.

Reviews

- There is no requirement to regularly review filtering and monitoring specifically, but safeguarding practice should be audited at least annually and there should be an annual review of safeguarding policies.[191]

Other

- There is no specific requirement to engage with parents when setting online safety policies, but child protection / safeguarding policies should be made available to parents.[192]
- Estyn inspections should verify schools' ability to recognise, respond to and resolve online safety issues.[193]

Scotland

What little guidance there is for Scottish schools comes from *The Scottish Government's National Action Plan on Internet Safety for Children and Young People*.[194]

Specifically with reference to the Prevent duty, this document says that "*Scottish specified authorities must ensure IT policies and IT filtering solutions are in place which limit access to terrorist and/or extremist material. Schools, colleges and universities are expected to have policies in place relating to the use of IT and to use filtering as a means of restricting access to harmful content. In addition both Further and Higher Education institutions must ensure they have clear policies and procedures for students and staff working on sensitive or extremism-related research.*"[195]

The guidance links to the UK Safer Internet Centre's *Appropriate Filtering for Education Settings* and *Appropriate Monitoring for* Schools guidance, although makes no other mention of them.[196]

190 *Keeping Learners Safe (Wales)*, ¶ 7.7.
191 *Keeping Learners Safe (Wales)*, ¶¶ 1.44, 2.9, 2.25.
192 *Keeping Learners Safe (Wales)*, ¶¶ 2.8, 2.26, 4.23.
193 *Keeping Learners Safe (Wales)*, ¶ 7.16.
194 *Internet Safety for Children and Young People (Scotland)*.
195 *Internet Safety for Children and Young People (Scotland)*, "Every child and young person has an age appropriate and evolving understanding of the opportunities and risks which exist in in the online world: Prevent Activity".
196 *Internet Safety for Children and Young People (Scotland)*, Annex D, "Regulation and Guidance".

There is also information about online safety, including education about online safety, in *The National Guidance for Child Protection In Scotland 2021*[197]. However, it makes no mention of filtering and monitoring.

Northern Ireland

Roles

- Whereas in England schools have a Designated Safeguarding Lead (DSL) (and deputies), in Northern Ireland these are known as the Designated Teacher (DT) and Deputy Designated Teachers (DDT).
- As well as the DT, a DDT is also explicitly required.[198]
- Schools should have a Safeguarding Team including the chair of the Board of Governors, Designated Governor for Child Protection, the Principal, the DT and DDT. Other people may be co-opted (e.g. SENCO, ICT Co-ordinator, etc.).[199]
- One or more designated members of staff should have a higher level of expertise around online safety.[200]

Training

- The staff training requirements are largely the same as in England, but the main guidance doesn't refer to **online** safety specifically and instead refers to safeguarding in general.[201] However, *DE Circular 2013/25* says that "*eSafety training is therefore an essential element of staff induction and should be part of an on-going Continuous Professional Development programme.*"[202]
- Governors' safeguarding training should be refreshed every 4 years.[203]
- DTs and DDTs should attend a two day "CPSS Introduction to Child Protection" course and a refresher every 3 years[204].

Teaching

- "*Research and advice indicates that, provided that those affordances are well understood by teachers and school leaders, and the deliberate use of digital tools, social communication environments and online resources which are easily accessed by mobile*

197 The Scottish Government, *National Guidance for Child Protection in Scotland*, 2021.
198 *Safeguarding and Child Protection in Schools (NI)*, §§ 3, 4.1, 4.2.4, 4.2.5, 4.3, Annex A.
199 *Safeguarding and Child Protection in Schools (NI)*, § 4.2.
200 *DE Circular 2016/27: Online Safety (NI)*, ¶ 9.
201 *Safeguarding and Child Protection in Schools (NI)*, § 4.1.
202 *DE Circular 2013/25: eSafety Guidance (NI)*, ¶ 4.1.i.
203 *Safeguarding and Child Protection in Schools (NI)*, § 4.1.
204 *Safeguarding and Child Protection in Schools (NI)*, § 4.7.2.

devices, is well prepared and planned, it can benefit learning and teaching inside and beyond the classroom."[205]

Filtering and Monitoring

- Northern Irish schools are also required to have filtering and monitoring,[206] but no guidance, such as the UK Safer Internet Centre's, is signposted. Filtering is usually done through Northern Ireland's C2k network, but schools can opt to buy an internet connection from a different service provider, and should implement their own filtering.[207]

Reviews

- The child protection policy should be reviewed annually, but the guidance does not mention *online* safety.[208]
- The anti-bullying policy should be reviewed every 4 years, and should integrate the online safety policy.[209]
- Safeguarding practices should be reviewed annually, and other safeguarding policies should be reviewed at least every 3 years and should integrate the online safety policy.[210]

Other

- Schools should have a child protection policy, which should reference the online safety policy.[211]
- Governors should receive an annual report on all child protection matters, but the guidance does not mention *online* safety.[212]
- All policies, including the online safety policy, should be issued to parents at intake and it is advisable to keep parents informed thereafter.[213]
- The online safety policy should be integrated into the safeguarding, behaviour, code of practice and anti-bullying policies, and should incorporate agreements on acceptable use of the internet, school based technology and personal mobile technology.[214]

205 The Department of Education (Northern Ireland), *DE Circular 2016/26: Effective Educational Uses of Mobile Digital Devices*, ¶ 2.
206 *Safeguarding and Child Protection in Schools (NI)*, § 6.8;
DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools (NI), ¶ 2.ii;
DE Circular 2013/25: eSafety Guidance (NI), ¶ 4.2.
207 *Safeguarding and Child Protection in Schools (NI)*, § 6.8;
DE Circular 2011/22: Internet Safety (NI), ¶¶ 2, 5, 8, Annex 2.ii, Annex2.viii.
208 *Safeguarding and Child Protection in Schools (NI)*, §§ 4.1, 4.3.1.
209 *Safeguarding and Child Protection in Schools (NI)*, §§ 4.1, 6.7.
210 *Safeguarding and Child Protection in Schools (NI)*, §§ 4.1 - 4.2, 6.7.
211 *Safeguarding and Child Protection in Schools (NI)*, §§ 3, 4.1, 4.3, Annex A.
212 *Safeguarding and Child Protection in Schools (NI)*, § 4.1.
213 *Safeguarding and Child Protection in Schools (NI)*, § 4.9;
DE Circular 2011/22: Internet Safety (NI), ¶ 11.
214 *Safeguarding and Child Protection in Schools (NI)*, § 6.7.

- Engage with parents to share information, advice and guidance on the appropriate and safe use of technology.[215]
- The guidance provides advice regarding sexting[216].
- Maintain a record of potential breaches of online safety in an Online Safety Risk Register[217].

215 *Safeguarding and Child Protection in Schools (NI)*, § 6.8;
DE Circular 2016/27: Online Safety (NI), ¶¶ 9, 17;
DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools (NI), ¶ 2.iii.
216 *Safeguarding and Child Protection in Schools (NI)*, § 6.9.
217 *DE Circular 2016/27: Online Safety (NI)*, ¶¶ 9, 17.

Bibliography

The Department for Education (England), *Buying for Schools*, 2023, https://www.gov.uk/guidance/buying-for-schools.

The Department for Education (England), *Cyber Security Standards for Schools and Colleges*, 2023, https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges.

The Department for Education (England), *Filtering and Monitoring Standards for Schools and Colleges*, 2023, https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges.

The Department for Education (England), *Keeping Children Safe in Education*, 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.

The Department for Education (England), *National Minimum Standards for Boarding Schools*, 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1160273/National_Minimum_Standards_for_boarding_schools.pdf.

The Department for Education (England), *Schools' Buying Strategy*, 2021, https://www.gov.uk/government/publications/schools-buying-strategy.

The Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, https://www.education-ni.gov.uk/sites/default/files/publications/education/Safeguarding%20%26%20Child%20Protection%20in%20Schools%20JUNE%202022.pdf.

The Department of Education (Northern Ireland), *DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools*, https://www.education-ni.gov.uk/publications/circular-200701-acceptable-use-internet-schools.

The Department of Education (Northern Ireland), *DE Circular 2011/22: Internet Safety, https://www.education-ni.gov.uk/publications/circular-201122-internet-safety*.

The Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, https://www.education-ni.gov.uk/publications/circular-201325-esafety-guidance.

The Department of Education (Northern Ireland), *DE Circular 2016/26: Effective Educational Uses of Mobile Digital Devices*, https://www.education-ni.gov.uk/publications/circular-201626-effective-educational-uses-mobile-digital-devices.

The Department of Education (Northern Ireland), *DE Circular 2016/27: Online Safety*, https://www.education-ni.gov.uk/publications/circular-201627-online-safety.

The Department of Education (Northern Ireland), *Education in Safe and Effective Practices*, https://www.education-ni.gov.uk/articles/education-safe-and-effective-practices.

Estyn, *Guidance for Inspectors*, 2022, https://www.estyn.gov.wales/system/files/2022-09/What%20we%20inspect%20-%202022_0.pdf.

The Information Commissioner's Office, *Recommended Actions in the Children's Code*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/best-interests-self-assessment/step-4-prioritise-actions/recommended-actions-in-the-children-s-code.

Ofsted, *School Inspection Handbook*, 2022, https://www.gov.uk/government/publications/school-inspection-handbook-eif/school-inspection-handbook#Evaluating%20personal%20development.

Ofsted, *The Safe Use of New Technologies*, 2010, https://webarchive.nationalarchives.gov.uk/ukgwa/20141105221831mp_/https://www.ofsted.gov.uk/sites/default/files/documents/surveys-and-good-practice/t/The%20safe%20use%20of%20new%20technologies.pdf.

Opendium, *Appropriate Filtering for Education Settings*, 2023, https://docs.opendium.com/wiki/Appropriate_Filtering_for_Education_Settings.

The Scottish Government, *Internet Safety for Children and Young People: National Action Plan*, 2017, https://www.gov.scot/publications/national-action-plan-internet-safety-children-young-people/.

The Scottish Government, *National Guidance for Child Protection in Scotland*, 2021, https://www.gov.scot/publications/national-guidance-child-protection-scotland-2021/.

The UK Safer Internet Centre, *Appropriate Filtering for Education Settings*, 2023, https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering.

The UK Safer Internet Centre, *Appropriate Monitoring for Education Settings: Substantive Changes*, 2023, https://d1xsi6mgo67kia.cloudfront.net/uploads/2023/05/Appropriate-Monitoring-for-Education-Settings-Substantive-Changes.pdf.

The UK Safer Internet Centre, *Appropriate Monitoring for Schools*, 2023, https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring.

The UK Safer Internet Centre, *Provider Responses,* https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/provider-responses.

United Kingdom General Data Protection Regulation, https://www.legislation.gov.uk/eur/2016/679/contents.

The Welsh Government, *Education Digital Standards for Schools in Wales: Web filtering*, 2021, https://hwb.gov.wales/support-centre/education-digital-standards/web-filtering-standards.

The Welsh Government (Wales), *Keeping Learners Safe*, 2022, https://www.gov.wales/sites/default/files/publications/2022-04/220401-keeping-learners-safe.pdf.