UK Online Safety Guidance in 2025

A Comprehensive Overview

Introduction

Whilst schools have long been required to do something "appropriate" when it comes to online safety, for many years the official guidance on the specifics was always very weak. In 2023, the Department for Education published the first edition of their *Filtering and Monitoring Standards for Schools and Colleges* guidance, which introduced the first official comprehensive guidance. If you are unfamiliar with those changes, we strongly recommend reading the *What's Changed* section of our 2023 overview.[1] Guidance has continued to evolve, and schools are expected to undertake a review of their filtering and monitoring provision at least once an academic year, to ensure that it continues to keep up with both technology and the latest guidance.

The 2025 edition of the Department for Education's *Keeping Children Safe in Education* statutory guidance was published in July 2025.[2] It signposted schools to guidance surrounding the use of Generative AI technologies, but did not include many other significant changes to online safety guidance. However, 2025 also saw parts of the *Online Safety Act*[3] come into force, which resulted in the UK Safer Internet Centre making significant changes to their *Appropriate Filtering for Education Settings*[4] and *Appropriate Monitoring for Schools*[5] guidance.

Education is devolved across the UK, with each nation having their own safeguarding and online safety guidance, with Education Wales introducing their new, more comprehensive, *Web filtering and online safeguarding* guidance.[6] However, of all the UK nations, the guidance for England is still 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 appendices.

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 online safety guidance from the multitude of separate documents, 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.

1 Opendium, *UK Online Safety Guidance in 2023*.
2 Department for Education (England), Keeping Children Safe in Education, 2025.
3 UK Government, *Online Safety Act 2023*.
4 UK Safer Internet Centre, *Appropriate Filtering for Education Settings*, 2025;
5 UK Safer Internet Centre, *Appropriate Monitoring for Schools*, 2025.
6 Education Wales (Wales), *Web filtering and online safeguarding, 2025.*

The scope of this document has been intentionally limited only to *online* safety. Safeguarding in general is a much broader subject, and beyond our remit as an online safety provider.

Who is Opendium?

Opendium is a small, specialist UK based online safety provider, who has been supplying UK schools for over 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.

> "*The support we receive from Opendium is absolutely formidable which sets them apart from others, Any time we've have had questions or needed assistance, their team is always there to support us, you are always able to speak to someone they has been quick to respond providing clear solutions and advice.*"
>
> — Stephen Hudd, Trust ICT Manager,
> Quantock Education Trust.

> "*Opendium consistently delivers outstanding service with a commitment to quality and customer satisfaction. Their expertise in web filtering and network consultancy is second to none, providing reliable, innovative products tailored to our needs.*"
>
> — Rob Wood, Assistant Network Manager,
> St. Oscar Romero Catholic School.

Opendium e-Safety

Table of Contents

What's Changed?

Since the previous update to the Department for Education's *Keeping Children Safe in Education,* in September 2024, there have been significant updates to online safety guidance for schools and colleges. These changes were introduced through the October 2024 update to the Department for Education's *Filtering and Monitoring Standards for Schools and Colleges*,[7] the June 2025 update to the UK Safer Internet Centre's *Appropriate Filtering for Education Settings*[8] and *Appropriate Monitoring for Schools*[9] and the July 2025 update to *Keeping Children Safe in Education*.[10]

The Welsh Government has also published *Web filtering and online safeguarding*, which contains much more comprehensive guidance than Welsh schools had previously been given.[11] These updates are documented in *Appendix A: Wales*.

Updates to Roles and Responsibilities

The Department for Education's guidance has always emphasised people working together, and the new guidance is no exception. It places more emphasis on the Designated Safeguarding Lead (DSL) and IT support working together, and the Senior Leadership Team's (SLT) and Governors providing support.[12]

The responsibility for buying filtering and monitoring systems has been clarified slightly: this is the Senior Leadership Team's (SLT's) responsibility,[13] with the IT provider helping with this task.[14]

Previously the guidance listed duties that the DSL "could" have, but this language has been strengthened and some additional responsibilities added. The DSL's responsibilities "should" now include:[15]

- checking relevant reports;
- responding to safeguarding concerns identified by filtering and monitoring;
- providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly. However, note that "reviewing the effectiveness of your provision" is listed as one of the SLT's responsibilities, so it is not clear who is ultimately responsible for conducting reviews;

7 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024.
8 UK Safer Internet Centre, *Appropriate Filtering for Education Settings*, 2025.
9 UK Safer Internet Centre, *Appropriate Monitoring for Schools*, 2025.
10 Department for Education (England), *Keeping Children Safe in Education*, 2025.
11 Education Wales (Wales), *Web filtering and online safeguarding, 2025.*
12 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Why this standard is important", ¶ 2.
13 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and The Department for Education (England), responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶ 1.
14 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2025, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶ 8.
15 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶¶ 5 – 6.

- making sure all users, parents and carers are aware of the school's policy;
- taking any necessary action in line with Keeping children safe in education and the school's existing safeguarding policies;[16] and
- any safeguarding and child protection matters that are identified through monitoring.[17] Previously the DSL took lead responsibility for this, whereas they now appear to have sole responsibility.

Whoever is assigned the responsibility for analysing logfile information should have sufficient capacity.[18]

Updates to Training

More emphasis has been placed on communicating with staff:

- how to deal with incidents;
- who should lead on any actions; and
- when incidents should be acted on, in line with the school's policy.

How these things are communicated with staff should be included as part of the school's monitoring plan.[19]

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:

- The UK Safer Internet Centre's definitions of categories that should be "managed" have received significant changes to bring them in line with the categories of illegal content which are now defined by the Online Safety Act. These are:[20]
  - child sexual abuse – content that depicts or promotes sexual abuse or exploitation of children, which is strictly prohibited and subject to severe legal penalties;
  - controlling or coercive behaviour – online actions that involve psychological abuse, manipulation, or intimidation to control another individual, often occurring in domestic contexts;

16 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶ 6.
17 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: How to meet the standard", ¶ 2.
18 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Monitoring Strategies: 2) Internet and web access", ¶ 1.
19 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard", ¶ 4.
20 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Illegal online content", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Illegal online content", ¶ 1.

- extreme sexual violence – content that graphically depicts acts of severe sexual violence, intended to shock or incite similar behaviour, and is illegal under UK law;
- extreme pornography – pornographic material portraying acts that threaten a person's life or could result in serious injury, and is deemed obscene and unlawful;
- fraud – deceptive practices conducted online with the intent to secure unfair or unlawful financial gain, including phishing and scam activities;
- racially or religiously aggravated public order offences – content that incites hatred or violence against individuals based on race or religion, undermining public safety and cohesion;
- inciting violence – online material that encourages or glorifies acts of violence, posing significant risks to public safety and order;
- illegal immigration and people smuggling – content that promotes or facilitates unauthorized entry into a country, including services offering illegal transportation or documentation;
- promoting or facilitating suicide – material that encourages or assists individuals in committing suicide, posing serious risks to vulnerable populations;
- intimate image abuse – the non-consensual sharing of private sexual images or videos, commonly known as “revenge porn”, intended to cause distress or harm;
- selling illegal drugs or weapons – online activities involving the advertisement or sale of prohibited substances or firearms, contravening legal regulations;
- sexual exploitation – content that involves taking advantage of individuals sexually for personal gain or profit, including trafficking and forced prostitution; and
- terrorism – material that promotes, incites, or instructs on terrorist activities, aiming to radicalise individuals or coordinate acts of terror.

Opinion: although it may be tempting to block all of the categories of illegal content, schools should be mindful of whether this is always appropriate due to the risk of over-blocking. As an example, if a student were to send a message to a member of staff in which they confide that they are considering suicide, it is possible that the message could be automatically categorised as "promoting or facilitating suicide" and blocked. In that situation, the filter would have directly endangered the life of the student. It is our opinion that schools should consider whether it is appropriate to exempt some or all staff from certain filters. Such exemptions could be restricted to certain devices or locations. For most of these categories, filters will be classifying content automatically, whereas the Internet Watch Foundation’s (IWF) and “police assessed list of unlawful terrorist content, produced on behalf of the Home Office” (CTIRU) block lists generally block very specific content and are reviewed by humans. As such, the IWF and CTIRU block lists have a very high efficacy

and low risk of false positives, and it not be possible for anyone within the school (including by the system administrator) to disable these.[21]

- The UK Safer Internet Centre's guidance continues to list some categories of "*inappropriate online content*"[22] in addition to the new categories of illegal content. Previously, there were some differences between the categories listed in the filtering guidance and those listed for monitoring, but most of these differences have now been eliminated. With the exception of the "Piracy and copyright theft" category, which is still only listed in the filtering guidance, the filtering and monitoring guidance now share a single list of categories. These are the notable changes this year:
  - The "Discrimination" and "Hate speech" categories have been merged into a single category.
  - The "Self-Harm" and "Suicide" categories have been merged into a single category. Previously they were listed as separate categories in the monitoring guidance.
  - The "Violence" category from previous guidance overlaps with the new categories of illegal content, and has been replaced with a "Violence Against Women and Girls (VAWG)" category, which has a much wider remit. The VAWG category covers content that "*promotes or glorifies violence, abuse, coercion, or harmful stereotypes targeting women and girls, including content that normalises gender-based violence or perpetuates misogyny.*"
  - The "Bullying" category from the previous monitoring guidance has been absorbed into a new "Harmful content" category, which applies to both filtering and monitoring. This is defined as "*Content that is bullying, abusive or hateful. Content which depicts or encourages serious violence or injury. Content which encourages dangerous stunts and challenges; including the ingestion, inhalation or exposure to harmful substances.*"
  - A number of categories that were listed as inappropriate content in the previous guidance overlap with the new categories of illegal content, and are therefore no longer listed separately under the "Inappropriate Online Content" heading. These are: "Child Sexual Exploitation, "Drugs / Substance abuse" and "Extremism". Note that the descriptions of the categories of illegal content that have replaced these categories do not fully capture the nuance of the previous descriptions. For example, previously content which "displays or promotes" the use of drugs was covered, whereas now it is only "advertisement and sale".
- Schools should consider whether their filtering and monitoring systems allow the configuration of restrictions and monitoring to be personalised for individual users by

21 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 1;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Illegal online content", ¶ 3.

22 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Inappropriate online content", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Inappropriate online content", ¶ 1.

identifying the user or device.[23] Filtering systems may need to be different, or set up differently for different user types, year groups and subjects, and should not have a blanket profile for all users. As a minimum, staff and students should have different levels of filtering.[24] When shared devices are used, users should log in individually so that monitoring systems can apply configurations based upon user profiles.[25]
Opinion: The need for users to log in to shared devices individually is only mentioned within the monitoring guidance. However, the filtering guidance also expects it to be possible for filtering systems to be personalised to individual users. Requiring users to log in would therefore appear to be equally important for both filtering and monitoring purposes, in order to support the requirements for personalisation.

- Schools should consider whether the filtering and monitoring systems will integrate with their safeguarding and wellbeing systems to better understand the context of a user's activities.[26]

Updates to Filtering

In addition to the changes listed in the *Updates to Filtering and Monitoring* section above:

- For several years, the UK Safer Internet Centre's guidance has required filtering systems to prevent schools (including their IT staff) from being able to disable the Internet Watch Foundation's (IWF's) block list and "the police assessed list of unlawful terrorist content, produced on behalf of the Home Office" block list (more commonly known as the Counter Terrorism Internet Referral Unit, or CTIRU, list). This requirement has now been incorporated into the DfE's guidance together with ensuring that the filtering provider regularly updates these block lists.[27]
Opinion: although filtering providers can remove the ability for a system administrator to disable or override specific categories, it is often impossible to prevent a suitably determined system administrator from completely bypassing the whole filtering system. The nature of a system administrator's job gives them unprecedented levels of access over the school systems, both in terms of software configuration but also physical access to parts of the school's network, including those parts that are on the "unfiltered internet side" of any filtering system.

- The ability for schools to permit or deny specific content themselves has previously been listed in the UK Safer Internet Centre's guidance, but this is now also in the DfE's guidance:

23 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.
24 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: How to meet the standard", ¶ 1 – 2.
25 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, 2025, "AC2", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.
26 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.
27 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶¶ 1 – 2;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Illegal Online Content", ¶ 2.

"*Some schools and colleges may want to block additional, inappropriate content that their filtering system does not automatically block. Your system should allow you to add this content locally. Any additions should not disrupt or affect teaching and learning.*"[28]

- The list of things that filtering should apply to has been updated slightly:[29]
  - "school owned devices" has been changed to "school managed devices"; and
  - school managed devices which are taken off-site should now be filtered (this was previously included in the UK Safer Internet Centre's guidance, but has now also been added to the DfE's).
- School-managed and unmanaged devices should be separated onto different virtual networks (VLANs).[30]
- Alerting has been made more specific – previously filtering systems were expected to alert when "*any web content has been blocked*", but as we noted in the 2023 edition of this document, filtering systems may block large amounts of incidental content, such as advertising, which is of no safeguarding concern. This has now been clarified such that filtering systems should alert "*when web content of concern has been blocked.*"[31]
- The DfE's guidance previously expected filters to identify and block technologies such as VPNs and proxy services, which could be used to circumvent the filtering, and now end-to-end encryption methods has been added to that list. Schools are encouraged to ask their IT support or filtering provider to block these technologies at a "system level".[32]
  Opinion: Messaging apps such as WhatsApp use end-to-end encryption, and can be used for both innocent or nefarious purposes. It is not possible to identify and block the "bad" uses of WhatsApp whilst allowing the "good" uses. Schools may want to conduct a risk assessment and decide whether the benefits outweigh the risks of allowing such apps. This is particularly relevant to boarding schools, who have a requirement to provide "appropriate internet access" for "social purposes,"[33] and where parents would expect to be able to keep in touch with their children. In many cases, students are likely to use these messaging apps regardless, using mobile data if necessary, but allowing access to them on

28 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2025, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 3;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1.

29 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 4.

30 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 5.

31 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 5.

32 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 5 – 6.

33 Department for Education (England), *National Minimum Standards for Boarding Schools*, 2022, ¶ 4.2.

the school network could encourage the use of the school's wifi, with its associated protections for other types of traffic.

- Schools should ask their IT support or filtering provider to ensure that networks and clients are appropriately configured (this includes firewalls, browsers and operating systems).[34]
- The UK Safer Internet Centre's guidance previously expected "Safe Search" to be enforced on search engines, whereas the DfE's guidance left this as a choice for the SLT. The DfE's guidance now more closely matches the UK Safer Internet Centre's and states that Safe Search should be enabled by default.[35]
- The DfE guidance also says to "*make sure that your safe search engine is locked into your chosen browser and cannot be changed*".[36] We're not entirely sure what this means – it could mean that the school should make a decision to use a specific search engine and set the browser's search box to use only that search engine, but this wouldn't add much protection since the user could simply go directly to their chosen search engine rather than using the browser's search box. Alternatively, it may mean that access to alternative search engines should be completely prevented, but that would surely be a job for the school's filter, not a browser configuration.
- Users should not be able to download additional browsers or unauthorised plugins.[37]
- If the filtering is provided by the internet service provider, schools should ask them how it meets the requirements.[38]
  Opinion: the UK Safer Internet Centre invites filtering providers to submit responses detailing how products meet their guidance, and these are published through their website.[39] When making a purchasing decision, and as part of their online review, it would be wise for schools to use these responses to evaluate suppliers. However, there are a few points that we feel should be considered:
  - *It is important to check the date of the response, since the guidance and technologies are constantly changing. If a filtering provider has not submitted a response recently, a school won't be able to properly assess their filtering in the context of the current standards.*

34 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 6.
35 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 12.
36 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 12.
37 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 12.
38 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 13.
39 UK Safer Internet Centre, *Provider Responses*.

- *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.*
- *The UK Safer Internet Centre has also started independently accrediting providers, which should be helpful to schools in the longer term. However, the accreditation process is being done gradually in small batches, so schools should be aware that many providers are currently unaccredited simply because the UK Safer Internet Centre hasn't got around to them yet.*

- The UK Safer Internet Centre's guidance no longer references network-level filtering in isolation, but that schools might consider combining network-level and device-level filtering.[40]

Updates to Monitoring

In addition to the changes listed in the *Updates to Filtering and Monitoring* section above:

- The DfE now offers a non-exhaustive list of criteria that will affect which solution the school chooses:[41]
  - student age;
  - student risk profile;
  - whether screens are easy to see;
  - number of devices in use; and
  - whether devices are used off-site, for example, at home.
- All staff should conduct a level of in-person monitoring if they are in a room with students on devices, as part of wider classroom supervision. Some schools and colleges may decide to have additional technical monitoring solutions (monitoring software installed on the individual devices) in place to reduce any risks identified during the review.[42]
- "*Live supervision by staff on a console with device management software*" is no longer listed as a potential monitoring strategy.[43]
- Schools and colleges should have a monitoring plan, which includes, as a minimum[44]:

40 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1.
41 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Why this standard is important", ¶ 2.
42 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: How to meet the standard", ¶ 1.
43 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 1.
44 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 1.

- how students are to be monitored (e.g. "*device monitoring using device management software*", "*in-person monitoring in the classroom*", or "*network monitoring using log files of internet traffic and web access*");[45]
- weekly monitoring reports highlighting incidents.[46]
- immediate reports when an incident is classed as high-risk (e.g. malicious, technical or safeguarding);[47] and
- how to communicate with staff about how to deal with incidents, who should lead on any actions, and when incidents should be acted on.[48]

- Everyone using the school network should know that they are being filtered and monitored, and monitoring systems should notify users that they are being monitored, such as by displaying a message every time they log in.[49]
- Schools should have a documented process for recording incidents that includes what action was taken and the outcomes."[50]
- Previously, the DfE's guidance required monitoring systems to be able to identify guest accounts. However, this has proved to be challenging for a lot of schools and the guidance has been relaxed to do this "where possible".[51]
- The UK Safer Internet Centre's guidance[52] no longer lists any requirement for schools to be prevented from disabling monitoring of certain categories of content. However, the text in their *Summary of Substantive Changes* document suggests that this may be an error.[53]
- Schools need to be aware of privacy concerns related to any monitoring of BYOD devices that occurs beyond school hours and location. Remote monitoring should concentrate on school-owned and managed devices.[54]
- Schools should understand to what extent their monitoring system can monitor content on mobile and web apps, and any configuration or extra components required to do this.[55]

45 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 1.
46 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 2.
47 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 2.
48 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 4.
49 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 3.
50 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 5.
51 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 8.
52 UK Safer Internet Centre, *Appropriate Monitoring*, 2025.
53 UK Safer Internet Centre, *Summary of Substantive Changes*, 2025, p 3
54 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.
55 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.

Updates to Reviews

- Reviews now need to be carried out at least "*once every academic year*" rather than "*annually*".[56] Also, in addition to the triggers listed previously, reviews need to be conducted when major software updates occur or when there are changes to the network or devices.[57]
- The guidance now notes that, in order to carry out a review, you will need to understand the technical limitations of your filtering system, such as whether it can filter real time content; any relevant serious incidents; how the school uses generative AI tools; and any technical set-up recommendations (presumably made by the filtering and monitoring providers).[58]
- Following system or equipment changes, schools should seek assurance that all filtering and monitoring solutions will continue to work on all school-managed devices.[59]
  Opinion: filtering and monitoring should be considered while schools are planning system and equipment changes, and the provider should be consulted at that time. If this assurance and guidance is not sought from filtering and monitoring providers before undertaking changes then the school risks being put in a position where a choice must be made between retiring brand new equipment immediately in order to properly safeguard the students, or unsafely using new equipment that has already been purchased. It may be necessary to reverse changes to systems systems if, following completion of the work, it is discovered that they are incompatible with the filtering or monitoring systems. Furthermore, when undertaking changes to your systems, the school's provider may be able to suggest work that could be undertaken at the same time with minimal additional effort that would significantly improve safeguarding opportunities. Schools should not assume that a networking contractor understands the requirements of their filtering system – always involve the filtering provider during the planning stage.
- Schools will need to investigate any risks or problems that the review identifies. Issues may be resolved by reviewing configuration, or the filtering and monitoring provision. However, it may be necessary to stop using the devices in question.[60]

Updates to Generative AI

For the first time, schools have been given some guidance on how to approach the use of Generative AI. Please see "Generative AI", below, for details about the Generative AI guidance.

56 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Why this standard is important", ¶ 2;
Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: How to meet the standard", ¶ 1;
Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 5.

57 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 5.

58 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 2.

59 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 4.

60 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 6.

Other Updates

- Misinformation and conspiracy theories are now included in the list of safeguarding harms associated with "content" risks.[61] "Fake news" (disinformation) was already listed in the previous guidance.
- "*Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement.*"[62]
- The Department for Education's *plan technology for your school service* is now sign posted, to help schools to self-assess themselves against the filtering and monitoring standards.[63]

61 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶ 135.
62 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶ 136.
63 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶ 142;
See also:
- Department for Education (England), *Plan Technology for your School*.

Overview of the Current Guidance

This section will concentrate on 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 appendices.

Opinion: A school's approach to online safety is expected to be risk based. There is therefore flexibility, and schools should not see the guidance as a rigid set of rules that they must comply with at all costs. However, where a school has decided to deviate from the guidance, they should have conducted and documented a thorough risk assessment so that they can show that they 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, outdated network designs, etc.)

Opinion: the UK Safer Internet Centre invites filtering providers to submit responses detailing how products meet their guidance, and these are published through their website.[64] When making a purchasing decision, and as part of their online review, it would be wise for schools to use these responses to evaluate suppliers. However, there are a few points that we feel should be considered:

- *It is important to check the date of the response, since the guidance and technologies are constantly changing. If a filtering provider has not submitted a response recently, a school won't be able to properly assess their filtering in the context of the current standards.*
- *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.*
- *The UK Safer Internet Centre has also started independently accrediting providers, which should be helpful to schools in the longer term. However, the accreditation process is being done gradually in small batches, so schools should be aware that many providers are currently unaccredited simply because the UK Safer Internet Centre hasn't got around to them yet.*

Data Protection

- Schools are the data controller of the personal data collected by their filtering (and presumably, monitoring) systems.[65]

64 UK Safer Internet Centre, *Provider Responses*.
65 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Inappropriate Online Content", ¶ 3.

- A Data Protection Impact Assessment (DPIA) should be conducted regarding the data collected by a school's filtering and monitoring systems and strategies.[66]
- Review the privacy notices of third party providers.[67]
- Ensure that there are sharing or processing agreements with your filtering and monitoring providers.[68] It is worth noting that Article 28 of the UK GDPR requires there to be data processing or sharing agreements with *any* third parties, such as employers of outsourced IT staff who have access to personal data pertaining to the school's staff or students.[69]
- Understand the school's filtering and monitoring provider's data retention policies.[70]
- Understand what data the monitoring (and presumably, filtering) system stores, and where it is stored (cloud / on-premises) and whether it is backed up.[71]
- Ensure that users understand that their online access is being monitored and that expectations of appropriate use are communicated and agreed. Monitoring systems should notify users that they are being monitored, such as by displaying a message every time they log in.[72] Users who are working remotely should be 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.[73]

66 Department for Education (England), *Filtering and Monitoring Standards, 22 October 2024*, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 10;
Department for Education (England), *Filtering and Monitoring Standards, 22 October 2024*, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 13;
UK Safer Internet Centre, *Appropriate Filtering, 2025*, "Inappropriate Online Content", ¶ 5;
UK Safer Internet Centre, *Appropriate Monitoring, 2025*, ¶ 3.

67 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 10.

68 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Inappropriate Online Content", ¶ 3;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, ¶ 3.

69 UK Government, United Kingdom General Data Protection Regulation, Article 28.

70 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Inappropriate Online Content" ¶ 3;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring strategies: 2) Internet and web access";
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.

71 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.

72 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 3;
Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.7;
Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, 06 December 2013, ¶¶ 4.2 – 4.3;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.

73 Information Commissioner's Office, *Recommended Actions in the Children's Code*, "Privacy information and community standards".

Roles and Responsibilities

The guidance specifies who holds the various responsibilities, but also emphasises that people should be working together, rather than in isolation, to fulfil these responsibilities[74].

- The Designated Safeguarding Lead (DSL) and IT support should work together, with the Senior Leadership Team's (SLT) and Governors providing support.[75]
- There should be a member of the Senior Leadership Team (SLT) and a governor responsible for ensuring that filtering and monitoring standards are met.[76] The responsible governor should be involved in reviews of the filtering and monitoring provision.[77]
- Whoever is assigned the responsibility for analysing logfile information should have sufficient capacity.[78]

Governing Bodies / Proprietors / Governors

Governing bodies, proprietors and governors are responsible for:[79]

- ensuring that online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement;[80] and
- identifying and assigning the roles and responsibilities of staff and third parties (e.g. external service providers).[81] Identify who is responsible for mobile devices, and the filtering and monitoring systems, and ensure that the DSL is also aware.[82]

Senior Leadership Team (SLT)

The SLT are responsible for:[83]

74 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Why this standard is important", ¶ 2;
Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶ 3.

75 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Why this standard is important", ¶ 2.

76 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: How to meet the standard", ¶ 2;
Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶ 2.9.

77 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: How to meet the standard", ¶ 2.

78 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Monitoring Strategies: 2) Internet and web access", ¶ 1.

79 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶¶ 1 – 2.

80 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶ 136.

81 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: How to meet the standard", ¶ 2.

82 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering on mobile devices";
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring on mobile devices".

83 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶¶ 1 – 2.

- buying filtering and monitoring systems, with the help of the IT provider;
- 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 the filtering system allows notes to be recorded against allowed / blocked URLs, etc., use that facility as it will everyone to understand why a website was whitelisted or blocked when the system is later reviewed, in the event of an incident, or when migrating the configuration to a new system were the school to change provider in the future.
- reviewing the effectiveness of the filtering and monitoring, with the help of the IT provider and DSL (see *Reviews*, below). However, note that "providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly" is listed as one of the DSL's responsibilities, so it is not clear who is ultimately responsible for conducting reviews;
- overseeing reports; and
  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.

Designated Safeguarding Lead (DSL)

- There should be a Designated Safeguarding Lead (DSL), who should be a senior member of staff from the leadership team, but not the proprietor of the school.[84]
- The DSL should be given the additional time, funding, training, resources and support needed to carry out the role effectively.[85]
- The DSL (or a deputy) should always be available during school hours to discuss safeguarding concerns.[86]
- The DSL should take lead responsibility for safeguarding and online safety, which should include:[87]

84 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶ 102;
Department for Education (England), *Keeping Children Safe in Education, 2025,* Annex C (¶ 1);
Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, §§ 3, 4.1, 4.2.4, 4.2.5, 4.3, Annex A.

85 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶ 103;
Department for Education (England), *Keeping Children Safe in Education, 2025,* Annex C (¶ 2).

86 Department for Education (England), *Keeping Children Safe in Education, 2025,* Annex C (¶ 4).

87 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶¶ 5 – 6.

- checking relevant reports;
- responding to safeguarding concerns identified by filtering and monitoring;
- providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly (see *Reviews* and *Checks*, below). However, note that "reviewing the effectiveness of your provision" is listed as one of the SLT's responsibilities, so it is not clear who is ultimately responsible for conducting reviews;
- making sure all users, parents and carers are aware of the school's policy;
- taking any necessary action in line with *Keeping Children Safe in Education* and the school's existing safeguarding policies;[88]
- any safeguarding and child protection matters that are identified through monitoring;[89] and
- helping the SLT to buy filtering and monitoring systems.[90]

IT Service Provider

The school's IT service provider may be a staff technician or an external service provider.[91]

They are responsible for:[92]

- maintaining filtering and monitoring systems;
- providing filtering and monitoring reports;
  Opinion: Usually the IT staff would configure the systems to regularly send suitable automated reports to appropriate staff.
- completing actions following concerns or system checks;
- helping the SLT to buy systems;
- working with the SLT and DSL to identify risk;
- working with the SLT and DSL to carry out reviews (see *Reviews*, below);
- working with the DSL to carry out checks (*Checks*, below); and

88 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶ 6.
89 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: How to meet the standard", ¶ 2.
90 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶ 8.
91 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶ 3.
92 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Identify and assign roles and responsibilities to manage your filtering and monitoring systems: Technical requirements to meet the standard", ¶¶ 6 – 7; Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 3.

- recording and reporting safeguarding concerns to the DSL (if the IT provider is responsible for managing device monitoring).[93]

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.[94]
- Separate training may be needed for governors and trustees, since they are involved in setting and testing safeguarding policies. "*This training should equip them with the knowledge to provide strategic challenge to test and assure themselves that the safeguarding policies and procedures in place in schools and colleges are effective and support the delivery of a robust whole school approach to safeguarding.*"[95]
- Training should be updated regularly.[96] In particular, the DSL's (and deputies') training should be updated at least every 2 years, such that they:[97]
    - "*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.*"
- In addition to formal training, the DSL's knowledge and skills should be updated at regular intervals, as required, and at least annually.[98]
- Training should be in line with any advice from safeguarding partners.[99]
- 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.*"[100]

93 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 3.
94 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶¶ 12, 124 – 125, Annex A (¶ 3);
Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶¶ 2.5, 2.34, 3.8;
Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 4.1;
Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, 06 December 2013, ¶ 4.1.i.
95 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶ 79;
Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶¶ 2.5, 2.11.
96 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶¶ 12, 79, 124 – 125, Annex A (¶ 1);
Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶¶ 2.5, 2.36, 3.8;
Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 4.1.
97 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶ Annex C (¶ 14).
98 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶ Annex C (¶ 15).
99 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶ 124.
100 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶ 126.

- Regular safeguarding / child protection / online safety updates should be sent to all staff (via email, e-bulletins, staff meetings, etc.) as required, at least annually.[101]
- Staff should have an awareness that technology is a significant component in many safeguarding / well being issues.[102]
- 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.[103] In particular, staff should have an understanding of how to respond to incidents, including the following details, and how this is communicated to staff should be documented in the school's monitoring plan:[104]
    - how to deal with incidents;
    - who should lead on any actions; and
    - when incidents should be acted on, in line with the school's policy.
- The DSL and IT staff may need to ask filtering and monitoring providers for system-specific training and support.[105]
  Opinion: Far too often, DSLs relay discussions through the IT staff instead of talking directly to providers.
- If the IT provider is responsible for managing device monitoring, they should receive safeguarding training which includes online safety.[106]

Teaching

- Schools have a responsibility to 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).[107] *Keeping Children Safe in*

101 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶¶ 12, 124, Annex A (¶ 3);
Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶ 3.6.
102 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶¶ 22, 24, 30, 33, 156, Annex A (¶ 3);
103 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶ 141;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC4", ¶ 4.
104 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school or college: Technical requirements to meet the standard", ¶ 4.
105 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: How to meet the standard", ¶ 3;
Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: How to meet the standard", ¶ 3.
106 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 7.
107 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶¶ 128, 132;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC4", ¶¶ 4 – 5;
Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.7;
Department of Education (Northern Ireland), *Education in Safe and Effective Practices*;
Department of Education (Northern Ireland), *DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools*, 16 July 2007, ¶ 2;
Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, 06 December 2013, ¶ 2.5;
Department of Education (Northern Ireland), *DE Circular 2016/27: Online Safety*, 01 December 2016, ¶¶ 9, 17
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 3;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 3.

Education links to various resources for teaching online safety. This also makes up part of the inspection frameworks published by Ofsted, the Independent Schools Inspectorate, and Estyn.[108]

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:

- Schools should have "appropriate" filtering systems and monitoring strategies to limit children's exposure to risks.[109]
- The Department for Education's *Schools' Buying Strategy* and *Buying for Schools* advice is signposted.[110] 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 provider was not providing a high enough level of support.
- Carry out a risk assessment and use it to inform filtering and monitoring provision.[111]
- Filtering systems and monitoring strategies should also be applied to guests, who should be identifiable where possible.[112]

108 Ofsted (England), *School Inspection Handbook*, 2022, ¶¶ 338 – 339, 349;
Independent Schools Inspectorate, *Handbook for the inspection of associated independent schools, including residential (boarding) schools and registered early years settings*, 2024, ¶ 137
Estyn (Wales), *Guidance for Inspectors: What we inspect – Maintained schools and PRUs*, 2023, § 3.1.

109 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶¶ 138, 141;
Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶ 7.7;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "Overview", ¶ 2;
Scottish Government (Scotland), *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";
Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.8;
Department of Education (Northern Ireland), *DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools*, 16 July 2007, ¶ 2.ii;
Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, 06 December 2013, ¶ 4.2.

110 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶ 143;
See also:
- The Department for Education (England), *Schools' Buying Strategy*, 2021.
- The Department for Education (England), *Buying for Schools*, 2025.

111 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶ 141;
Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.8;
Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, 06 December 2013, ¶ 4.1.iii;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Risk Assessment", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Risk Assessment", ¶ 1.

112 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2025, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 4;
Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 8;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC2", ¶ 2;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC3", ¶ 1.

- Filtering and monitoring should handle multilingual web content, images, common misspellings and abbreviations.[113]
- Filtering and monitoring should be "*context appropriate*" based on age, ability, vulnerability and risk of harm and should not have a blanket filtering profile for all users. As a minimum, staff and students should have different levels of filtering. Schools should consider whether their filter and monitoring systems allow the configuration of restrictions and monitoring to be personalised for individual users.[114]
- Schools should be able to control filtering and monitoring systems themselves in order to permit or deny access to specific content, and be able to change the keywords which the monitoring system uses to trigger alerts, without disrupting teaching and learning.[115]
  Opinion: It is important for schools to be able to control their own systems so that they 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" for their products, which tell schools that they must whitelist huge services such as Amazon Web Services (AWS), or Cloudflare. If a school were to blindly follow those instructions they would endanger their children, whereas the filtering provider would easily spot the danger and be able to help put together a safer configuration.
- 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*".[116]
- The filtering system and monitoring strategy should be able to manage the following categories of content at a minimum:[117]

Category	Filtering	Monitoring

113 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 5;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC1", ¶ 2;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.

114 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: How to meet the standard", ¶ 1.
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.

115 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2025, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 3;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.

116 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.

117 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Illegal online content", ¶ 1;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Inappropriate online content", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Illegal online content", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Inappropriate online content", ¶ 1.

Illegal online content (defined by the Online Safety Act)		
Child sexual abuse	✓	✓
Controlling or coercive behaviour	✓	✓
Extreme sexual violence	✓	✓
Extreme pornography	✓	✓
Fraud	✓	✓
Racially or religiously aggravated public order offences	✓	✓
Inciting violence	✓	✓
Illegal immigration and people smuggling	✓	✓
Promoting or facilitating suicide	✓	✓
Intimate image abuse	✓	✓
Selling illegal drugs or weapons	✓	✓
Sexual exploitation	✓	✓
Terrorism	✓	✓
Inappropriate online content		
Gambling	✓	✓
Hate speech / discrimination	✓	✓
Harmful content	✓	✓
Malware / hacking	✓	✓
Misinformation / disinformation	✓	✓
Piracy and copyright theft	✓	
Pornography	✓	✓
Self-harm and eating disorders	✓	✓
Violence against women and girls (VAWG)	✓	✓

Notes:

- Blocking content identified as illegal child sexual abuse material (CSAM) by the Internet Watch Foundation (IWF), or as unlawful terrorist content by the “Police Assessed List of Unlawful Terrorist Content, Produced on Behalf of the Home Office” (Counter-Terrorism Internet Referral Unit – CTIRU) is mandatory and it must not be possible for anyone within the school, including the system administrator, to override or disable these block lists.[118]
  Opinion: although filtering providers can remove the ability for a system administrator to

118 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 1;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, “Illegal online content”, ¶ 3.

disable or override specific categories, it is often impossible to prevent a suitably determined system administrator from completely bypassing the whole filtering system. The nature of a system administrator's job gives them unprecedented levels of access over the school systems, both in terms of software configuration but also physical access to parts of the school's network, including those parts that are on the "unfiltered internet side" of any filtering system.

- The name of the "Harmful content" category seems quite non-descriptive, given that pretty much all of the categories can be considered to be "harmful". The description of this category is "*Content that is bullying, abusive or hateful. Content which depicts or encourages serious violence or injury. Content which encourages dangerous stunts and challenges; including the ingestion, inhalation or exposure to harmful substances.*"
- *Opinion: although it may be tempting to block all of the categories of illegal content, schools should be mindful of whether this is always appropriate due to the risk of over-blocking. As an example, if a student were to send a message to a member of staff in which they confide that they are considering suicide, it is possible that the message could be automatically categorised as "promoting or facilitating suicide" and blocked. In that situation, the filter would have directly endangered the life of the student. It is our opinion that schools should consider whether it is appropriate to exempt some or all staff from certain filters. Such exemptions could be restricted to certain devices or locations. For most of these categories, filters will be classifying content automatically, whereas the Internet Watch Foundation's (IWF) and "police assessed list of unlawful terrorist content, produced on behalf of the Home Office" (CTIRU) block lists generally block very specific content and are reviewed by humans. As such, the IWF and CTIRU block lists have a very high efficacy and low risk of false positives, and as noted above, it must not be possible to for anyone within the school to disable these.*

- Schools 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.[119] In particular, some technologies cannot be monitored using other strategies (e.g. images or videos taken on mobile devices or from cloud storage).[120]
- Schools should consider whether their filtering and monitoring systems have the ability to deploy a central policy to multiple schools, and to have a centralised dashboard providing oversight.[121]

119 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Why this standard is important", ¶ 2;
Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 11;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "Overview", ¶ 2;
Department of Education (Northern Ireland), *DE Circular 2011/22: Internet Safety*, 27 September 2011, ¶ 4.;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, ¶ 6;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Content", ¶ 1.
120 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "1) Physical Monitoring", ¶ 2;
121 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1;

Opinion: Whether this is important functionality depends upon whether the school is 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**).[122]
  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.[123]

- Identify vulnerable users of mobile devices, paying particular attention to ensure that harmful content is not accessible on specific devices.[124]

- Schools should consider whether their filtering and monitoring systems allow the configuration of restrictions and monitoring to be personalised for individual users by identifying the user or device.[125] Filtering systems may need to be different, or set up differently "*for different user types, year groups and subjects*",[126] and "*should not have a blanket profile for all users*". As a minimum, staff and students should have different levels of filtering.[127] When shared devices are used, users should log in individually so that monitoring systems can apply configurations based upon user profiles.[128]
  Opinion: The need for users to log in to shared devices individually is only mentioned within the monitoring guidance. However, the filtering guidance also expects it to be possible for filtering systems to be personalised to individual users. Requiring users to log in would therefore appear to be equally important for both filtering and monitoring purposes, in order to support the requirements for personalisation.

- Schools should consider whether the filtering and monitoring systems will integrate with their safeguarding and wellbeing systems to better understand the context of a user's activities.[129]

UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.

122 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 2;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 2.

123 Opendium, *Appropriate Filtering for Education Settings*, "Capacity".

124 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering on Mobile devices";
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring on Mobile devices".

125 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.

126 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: How to meet the standard", ¶ 1.

127 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: How to meet the standard", ¶ 2.

128 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.

129 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.

Filtering

In addition to the requirements listed in the *Filtering and Monitoring* section above:

- Ensure that harmful and inappropriate content is blocked.[130] 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[131]. 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**.*"[132] Boarding schools may therefore have to provide access to social networks and encrypted communications apps such as Whatsapp. 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*".[133] One of the recommendations to come out of the report was that schools should "*manage the transition from locked down 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.*"[134]
- Schools need to understand the coverage of their filtering system, any limitations it has, and mitigate them to minimise harm.[135]
- The filtering provider should be an IWF member.[136]
- The filter should be operational and up to date.[137]

130 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Why this standard is important", ¶ 4;
Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.8.

131 Department for Education (England), *Keeping Children Safe in Education, 2025,* ¶ 133;
Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Why this standard is important", ¶ 4;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC3", ¶ 1;
Department of Education (Northern Ireland), *DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools*, 16 July 2007, ¶ 2.

132 Department for Education (England), *National Minimum Standards for Boarding Schools*, 2022, ¶ 4.2.

133 Ofsted (England), *The Safe Use of New Technologies*, 2010, p 5.

134 Ofsted (England), *The Safe Use of New Technologies*, 2010, p 6.

135 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Why this standard is important", ¶¶ 2 – 3.

136 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2025, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 2;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Illegal Online Content", ¶ 2.

137 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2025, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 2.

- The filter should incorporate, and regularly update, the Counter-Terrorism Internet Referral Unit (CTIRU) block list, or the Internet Watch Foundation's (IWF) child sexual abuse material (CSAM) block list.[138]
- Filtering should be applied to all:[139]
  - school managed devices (with remote school-owned devices receiving "*the same or equivalent filtering to that provided in school*"[140]);
  - unmanaged devices under a bring your own device (BYOD) scheme;
  - guests who have access to the school internet; and
  - all internet feeds, including backup connections and portable wifi devices.
- Circumvention attempts (e.g. VPNs, proxies and end-to-end encryption) should be identified and blocked. Schools are encouraged to ask their IT support or filtering provider to block these technologies at a "system level".[141]
  Opinion: The 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. Messaging apps such as WhatsApp use end-to-end encryption, and can be used for both innocent or nefarious purposes. It is not possible to identify and block the "bad" uses of WhatsApp whilst allowing the "good" uses. Schools may want to conduct a risk assessment and decide whether the benefits outweigh the risks of allowing such apps. This is particularly relevant to boarding schools, who have a requirement to provide "appropriate internet access" for "social purposes,"[142] and where parents would expect to be able to keep in touch with their children. In many cases, students are likely to use these messaging apps regardless, using mobile data if necessary, but allowing access to them on the school network could encourage the use of the school's wifi, with its associated protections for other types of traffic.

138 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶¶ 1 – 2;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Illegal Online Content", ¶ 2.

139 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2025, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶¶ 4 – 5;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC2", ¶ 2;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC3", ¶ 1.

140 Education Wales (Wales), *Digital Standards: Web filtering and online safeguarding*, 07 February 2025, "AC7", ¶ 1;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1.

141 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2025, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 5 – 6;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1.

142 Department for Education (England), *National Minimum Standards for Boarding Schools*, 2022, ¶ 4.2.

- Schools should ask their IT support or filtering provider to ensure that networks and clients are appropriately configured (this includes firewalls, browsers and operating systems).[143]
- The filtering system should provide alerts when web content of concern has been blocked.[144]
  Opinion: The way that the system alerts for different type of content 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 set up 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, the filtering system may routinely block a large amount of incidental content such as adverts from advertisers that are known to show harmful content.
- Get confirmation from the filtering provider as to whether they can filter "mobile" or "app" technologies.[145]
- The filtering system should allow the school to identify[146]:
  - device name or ID;
  - IP address;
  - the individual (where possible);
  - time and date of attempted access; and
  - the search term or content that was blocked.
- School-managed and unmanaged devices should be separated onto different virtual networks (VLANs).[147]
- The filtering system should be able to enforce search engines' "Safe Search" mode, or a child friendly search engine.[148]

143 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 6.
144 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2025, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 5;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC4", ¶ 2;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC5", ¶¶ 1, 3.
145 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2025, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 7;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1.
146 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2025, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 9;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1.
147 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 5.
148 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2025, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 9;

- The DfE guidance also says to "*make sure that your safe search engine is locked into your chosen browser and cannot be changed*".[149] We're not entirely sure what this means – it could mean that the school should make a decision to use a specific search engine and set the browser's search box to use only that search engine, but this wouldn't add much protection since the user could simply go directly to their chosen search engine rather than using the browser's search box. Alternatively, it may mean that access to alternative search engines should be completely prevented, but that would surely be a job for the school's filter, not a browser configuration.
- Users should not be able to download additional browsers or unauthorised plugins.[150]
- If the filtering is provided by the internet service provider, the school should ask them how it meets the requirements.[151]
  Opinion: the UK Safer Internet Centre invites filtering providers to submit responses detailing how products meet their guidance, and these are published through their website.[152] When making a purchasing decision, and as part of their online review, it would be wise for schools to use these responses to evaluate suppliers. However, there are a few points that we feel should be considered:
  - *It is important to check the date of the response, since the guidance and technologies are constantly changing. If a filtering provider has not submitted a response recently, a school won't be able to properly assess their filtering in the context of the current standards.*
  - *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.*
  - *The UK Safer Internet Centre has also started independently accrediting providers, which should be helpful to schools in the longer term. However, the accreditation process is being done gradually in small batches, so schools should be aware that many providers are currently unaccredited simply because the UK Safer Internet Centre hasn't got around to them yet.*

UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1.

149 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 12.

150 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", .

151 The Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 13.

152 UK Safer Internet Centre, *Provider Responses*.

- Staff should be aware of reporting mechanisms for both safeguarding and technical concerns and report if:[153]
    - 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;

    Opinion: It is important for staff to include as much detail as they can in their reports, such as the time that the incident happened, which user or device was involved, and if possible a screen shot of any "you have been blocked" message or other error. Given a school which may have 1000 devices using the internet concurrently, it is extremely hard for IT staff to act on a terse report such as "One of the students in my class was blocked from accessing a web page", whereas a report like "At 10:05, Joe Bloggs was using one of the workstations in IT room 1 and was blocked for pornography (screenshot attached)" would allow IT staff to quickly identify the offending traffic in the filter's logs.
- 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.[154]
- The filtering provider should publish a rationale that details their approach to filtering and over-blocking.[155]
- Schools should understand how their filtering system is deployed and may consider maximising combining network-level and device-level filters to maximise effectiveness.[156]
- There should be a way for users to report content which has been either over-blocked or under-blocked.[157]
- The filtering system should provide clear information on users' historical web browsing activity.[158]

Monitoring

In addition to the requirements listed in the *Filtering and Monitoring* section above:

153 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 14.
154 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC1", ¶ 1; UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1.
155 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1.
156 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1.
157 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1.
158 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering System Features", ¶ 1.

- Schools 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:[159]
  - device monitoring using device management software;
  - in-person monitoring by staff in the classroom; and
  - network monitoring using logs of internet and web traffic.
- Which strategies or solutions the school chooses will depend on this non-exhaustive list of criteria:[160]
  - student age;
  - student risk profile;
  - whether screens are easy to see;
  - number of devices in use;
  - whether devices are used off-site, for example, at home; and
  - whether a review identified any risks that the school decides should be reduced by an additional "technical monitoring solution" (monitoring software installed on the individual devices).[161]
- Whatever strategy the school chooses, all staff should conduct a level of in-person monitoring if they are in a room with students on devices, as part of wider classroom supervision.[162]
- The monitoring strategy should pick up incidents urgently, allowing the school to take prompt action and record the outcome.[163]
- Schools and colleges should have a monitoring plan, which includes, as a minimum[164]:
  - how students are to be monitored (e.g. "*device monitoring using device management software*", "*in-person monitoring in the classroom*", or "*network monitoring using log files of internet traffic and web access*");[165]

159 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategies", ¶ 1.
160 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Why this standard is important", ¶ 2.
161 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: How to meet the standard", ¶ 1.
162 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: How to meet the standard", ¶ 1.
163 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Why this standard is important", ¶ 3.
164 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 1.
165 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 1.

- weekly monitoring reports highlighting incidents.[166]
- immediate reports when an incident is classed as high-risk (e.g. malicious, technical or safeguarding);[167]
- how the school communicates with staff about how to deal with incidents, who should lead on any actions, and when incidents should be acted on;[168] and
- a documented process for recording incidents that includes what action was taken and the outcomes.[169]

- Ensure that monitoring data is in a format that staff can understand[170].
- Monitoring data needs to be regularly reviewed, interpreted and alerts prioritised.[171]
- Consider how are alerts are recorded, communicated and escalated.[172]
- The monitoring strategy should be able to identify users, including guests where possible.[173]
- Filtering systems may not pick up mobile or app content, so a "technical monitoring system" (monitoring software installed on the individual devices) should be applied to those devices.[174] Schools should understand to what extent their monitoring system can monitor content on mobile and web apps, and any configuration or extra components required to do this.[175]
- The monitoring system should identify and alert to the behaviours associated with each of the 4 areas of risk:[176]

166 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 2.
167 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 2.
168 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 4.
169 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 5.
170 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 8.
171 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategies: 2) Internet and web access", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.
172 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.
173 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 8;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategies: 2) Internet and web access", ¶ 1;
174 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning: Technical requirements to meet the standard", ¶ 7;
Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 9.
175 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.
176 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Have effective monitoring strategies that meet the safeguarding needs of your school of college: Technical requirements to meet the standard", ¶ 10;
Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶ 135;
Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.7.

  - content: illegal / inappropriate / harmful content – pornography, racism, misogyny, self-harm, suicide, anti-semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories;
  - contact: harmful interaction with other people – peer pressure, advertising, grooming / exploitation (for sex, crime, financial, etc.);
  - conduct: risky / harmful online behaviour – exchanging nudes / pornography, bullying; and
  - commerce: gambling, inappropriate advertising, phishing, scams.

- The school should be aware of any limitations of the logfile information produced by their filtering and monitoring systems.[177]
- Pro-active monitoring systems are available, whereby alerts are managed and supported by a third-party provider.[178] This relieves the school of some of the work and ensures that genuine threats to health and life are escalated. Ensure that the provider's SLA meets yhe school's requirements.
- If the school operates a BYOD (Bring Your Own Device) system, consider whether personal devices and apps can be monitored, and ensure it is deployed in accordance with the school's policies, including data protection. Schools need to be aware of privacy concerns related to any monitoring of BYOD devices that occurs beyond school hours and location. Remote monitoring should concentrate on school-owned and managed devices.[179]
  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.*
- 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 the school's requirements.[180]
- The monitoring system should detect harmful images. For example, using image hashes is one strategy, but different providers approach this in different ways.[181]
- Where users are working remotely, the school should understand the extent to which they are monitored while outside of the school premises.[182]

177 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategies: 2) Internet and web access", ¶ 1;
178 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategies: 3) Active/Pro-active technology monitoring services", ¶ 1;
179 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.
180 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.
181 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.
182 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.

- The school should have policies and processes to support those staff responsible for managing monitoring systems.[183]
  Opinion: In additional to any professional support necessary for staff to carry out their work, it is possible that staff may themselves be exposed to harmful content whilst reviewing logs and alerts, and may require emotional support, counselling, etc.

Reviews

- Regularly review the school's approach to online safety and the effectiveness of the filtering and monitoring provision, including redoing risk assessments.[184] The DfE's 'plan technology for your school' service, the 360 Safe website and LGfL online safety audit are all signposted.
- The review and risk assessment should be carried out.[185]
  - at least every academic year;
  - when a safeguarding risk is identified;
  - when working practices change (e.g. introduction of remote access, BYOD, etc.);
  - when new technology is introduced;
  - when major software updates occur;
  - when there are changes to the technical configuration of the network and devices; and
  - 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.[186]

183 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 2.
184 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶¶ 140, 142, 145;
Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶¶ 1.44, 2.9, 2.25, 7.4;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "Overview", ¶ 3;
Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, §§ 4.1 - 4.2, 4.3.1, 6.8, 6.9.2;
Department of Education (Northern Ireland), *DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools,* 16 July 2007, ¶ 1;
Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, 06 December 2013, ¶ 4.1.iii;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Risk Assessment", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Risk Assessment", ¶ 1;
See also:
- Department for Education (England), *Plan technology for your school*.
- South West Grid for Learning, *360 Degree Safe*.
- London Grid for Learning, *Online Safety Audit*.

185 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Why this standard is important", ¶ 2;
Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: How to meet the standard", ¶ 1;
Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 5;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 2;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Risk Assessment", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Risk Assessment", ¶ 1.
186 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Risk Assessment", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Risk Assessment", ¶ 1.

- The results of the review should be recorded.[187]
- To carry out the review the school needs to understand.[188]
    - the risk profile of pupils (ages, special needs / disabilities, whether English is a first or second language);
    - what the filter blocks / allows and why;
    - technical limitations, such as whether the school's solution can filter real time content;
    - 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);
    - how the school uses technologies, including Bring Your Own Device (BYOD) and generative AI tools;
    - the safeguarding / technology policies;
    - what checks are taking place and how resulting actions are handled (see *Checks*, below); and
    - any technical set-up recommendations to make sure the system works effectively.
- The review should inform:[189]
    - safeguarding and technology policies / procedures;
    - roles and responsibilities;
    - staff training;
    - curriculum and learning opportunities;
    - what checks are made and how often (see *Checks*, below);
    - monitoring strategies; and
    - procurement decisions.
- Following system or equipment changes, the school should seek assurance that all filtering and monitoring solutions will continue to work on all school-managed devices.[190]

187 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: How to meet the standard", ¶ 2.
188 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 2.
189 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 3.
190 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 4.

Opinion: filtering and monitoring should be considered while schools are planning system and equipment changes, and the provider should be consulted at that time. If this assurance and guidance is not sought from filtering and monitoring providers before undertaking changes then the school risks being put in a position where a choice must be made between retiring brand new equipment immediately in order to properly safeguard the students, or unsafely using new equipment that has already been purchased. It may be necessary to reverse changes to systems systems if, following completion of the work, it is discovered that they are incompatible with the filtering or monitoring systems. Furthermore, when undertaking changes to your systems, the school's provider may be able to suggest work that could be undertaken at the same time with minimal additional effort that would significantly improve safeguarding opportunities. Schools should not assume that a networking contractor understands the requirements of their filtering system – always involve the filtering provider during the planning stage.

- Inappropriate content that the school chooses to block should be reviewed and updated in line with changes to guidance and safeguarding risks.[191]
- 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.[192]
- Review security protection procedures periodically to keep up with evolving cyber-crime technologies.[193]
- Consider how monitoring reports inform the school's policy and practice?[194]
- The school will need to investigate any risks or problems that the review identifies. Issues may be resolved by reviewing configuration, or the filtering and monitoring provision. However, it may be necessary to stop using the devices in question.[195]

Checks

Whereas regular "reviews" are needed to ensure that policies and processes are remaining current, schools 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.[196]

191 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 11.
192 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶ 6;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering on Mobile devices", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring on Mobile devices", ¶ 1.
193 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶ 144.
194 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring Strategy/System Features", ¶ 1.
195 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 6.
196 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶¶ 8 – 9;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Checks and Documentation", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Checks and Documentation".

- Checks should include a range of:[197]
  - school owned devices and services, including those used off site;
  - locations across the site or sites, and off-site (where appropriate);
  - user groups, for example, teachers, pupils and guests; and
  - installed mobile apps (not just internet browsers).
- Carry out checks:
  - on new devices before they are distributed;[198] and
  - when significant changes have taken place (e.g. technology, policy or legislative changes).[199]
- For each check, document:
  - the date and time;
  - who did the check;
  - the location;
  - the device;
  - the user the check was performed as;
  - what was tested or checked; and
  - what the resulting actions were.[200]
- The SWGfL's testfiltering.com tool is signposted.[201]
  Opinion: although this is a good place to start, this tool only performs a few rudimentary checks. Schools 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

197 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 9;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 1;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Filtering on Mobile devices", ¶ 2;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring on Mobile devices", ¶ 2.

198 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 11.

199 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Checks and Documentation", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Checks and Documentation".

200 Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 10;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Checks and Documentation", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Checks and Documentation".

201 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶ 143;
Department for Education (England), *Filtering and Monitoring Standards*, 22 October 2024, "Review your filtering and monitoring provision at least annually: Technical requirements to meet the standard", ¶ 12;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 1;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Checks and Documentation", ¶ 2;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Monitoring on Mobile devices", ¶ 2;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Monitoring on Mobile devices", ¶ 2.

categories are filtered and monitored. Do not treat the results of testfiltering.com as a simple pass / fail, but instead check whether they match your policy. For example, if testfiltering.com shows that offensive language is not being blocked for staff, this is not a "failure" if your policy is to not block offensive language for staff (we would not recommend blocking offensive language for adults as it is likely to result in over-blocking).

Mobile Phones

The most pertinent points of the guidance for mobile phone use in school are given below. Please consult the guidance itself for more detail and how to achieve these policies.[202]

- 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.[203]
- Schools should develop a mobile phone policy, as part of their behaviour policy, that prohibits the use of mobile phones (and similar communications technology) throughout the school day, including during lessons, the time between lessons, breaktimes and lunchtime.[204]
- A Bring Your Own Device (BYOD) scheme may be offered to facilitate the use of laptops or tablets for learning, but this should not include mobile phones.[205]
  Opinion: The guidance does not specify whether this applies to both staff and students, or only students. Since it goes on to say that there are circumstances where it is appropriate for staff to use their mobile phones, we presume that allowing staff to use mobile phones as part of a BYOD scheme is allowed.
  Since boarding schools are expected to develop a policy for the use of mobile phones outside of the normal school day, and that "appropriate internet access, is provided for boarders for the purposes of organised and private study outside school hours and ***for social purposes****,"[206] it is likely that these are also circumstances where it is acceptable to include mobile phones within a BYOD scheme. With appropriate network level monitoring and filtering, children using the school's network are inherently safer than those using their personal mobile 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*

202 Department for Education (England), *Mobile phones in schools*, February 2024;
Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024;
Department of Education (Northern Ireland), *DE Circular 2024/14: Guidance for Schools on Pupils' Personal Use of Mobile Phones and other Similar Devices During the School Day*, 03 September 2024.
203 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶ 137.
Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, 06 December 2013, ¶ 5.3;
Department for Education (England), *National Minimum Standards for Boarding Schools*, ¶ 8.4.
204 Department for Education (England), *Mobile phones in schools*, February 2024, p 6, ¶ 1;
Department of Education (Northern Ireland), *DE Circular 2024/14: Guidance for Schools on Pupils' Personal Use of Mobile Phones and other Similar Devices During the School Day*, 03 September 2024, ¶¶ 4, 18, 21 – 22.
205 Department for Education (England), *Mobile phones in schools*, February 2024, p 6, ¶ 2.
206 Department for Education (England), *National Minimum Standards for Boarding Schools*, 2022, ¶ 4.2.

reasonable approach, but should be supported and documented by a robust risk assessment.

- The prohibition on mobile phones may be relaxed at limited times and locations for sixth form students (see the guidance for more details).[207]
- Staff should not use their own mobile phone for personal reasons in front of students during the school day. However, it may be appropriate for staff to use a mobile phone for professional reasons (e.g. for multi-factor authentication).[208]
- Schools have a duty to make reasonable adjustments where necessary, so may need to allow the use of mobile phones under some circumstances.[209]
- Schools should develop a policy on the use of mobile phones outside of the normal school day. For example, on school trips, or, in the case of boarding schools, at any other times. Policies should safeguard and promote the welfare of the students and avoid disruption to school trips.[210]
- Boarding schools should facilitate arrangements so that boarders can contact their parents and families in private, at a time suitable for both parties.[211]

Generative AI

The Department for Education's *Generative AI: product safety expectations* guidance is signposted.[212] However, this guidance is aimed at the vendors that are designing AI systems for schools and is of limited use to the schools themselves.

Guidance aimed at schools comes from the Department for Education's *Generative artificial intelligence (AI) in education* policy paper, and the UK Safer Internet Centre's *Appropriate Filtering for Education Settings* and *Appropriate Monitoring for Schools*.

- Filtering systems should effectively and reliably prevent access to harmful and inappropriate content generated by Generative AI systems.[213]
- Monitoring systems should maintain activity logs which capture the content created by generative AI tools.[214]

---

207 Department for Education (England), *Mobile phones in schools*, February 2024, p 6, ¶ 4;
Department of Education (Northern Ireland), *DE Circular 2024/14: Guidance for Schools on Pupils' Personal Use of Mobile Phones and other Similar Devices During the School Day*, 03 September 2024, ¶ 29.

208 Department for Education (England), *Mobile phones in schools*, February 2024, p 8, ¶ 3.

209 Department for Education (England), *Mobile phones in schools*, February 2024, p 10, ¶ 2;
Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, ¶ 19;
Department of Education (Northern Ireland), *DE Circular 2024/14: Guidance for Schools on Pupils' Personal Use of Mobile Phones and other Similar Devices During the School Day*, 03 September 2024, ¶¶ 26 – 28.

210 Department for Education (England), *Mobile phones in schools*, February 2024, p 6, ¶ 3; p 11, ¶ 3.

211 Department for Education (England), *Mobile phones in schools*, February 2024, p 6, ¶ 3.

212 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶ 143.
See also:
- Department for Education (England), *Generative AI: Product safety expectations*.

213 UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Generative AI Technologies", ¶ 1.

214 UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Generative AI Technologies", ¶ 1.

- Generative AI should only be used by pupils under close supervision, and with appropriate filtering and monitoring features.[215]
- Schools should assess which generative AI systems they wish to approve for use, taking into account safety and data protection features, and develop a policy around the use of generative AI by staff and students.[216]
    - they must comply with age restrictions set by the AI tools;
    - how to accommodate AI within their approach to online safety?;
    - ensure that their filtering and monitoring approaches can block and monitor dynamically generated content in real-time;
    - how well the safety features of AI systems that they wish to approve work;
    - how well the AI systems that they wish to approve meet data protection requirements;
    - how to meet their responsibilities regarding international property;
    - what ability do you have to generate reports on the usage of AI systems within the school.

    Opinion: The guidance is clear that AI use should not be a "free for all" – the school should evaluate the products that are available and decide which to approve for use by staff and students, with reference to the Department for Education's Generative AI: product safety expectations guidance. Generative AI tools are no longer just stand-alone web sites, and are often integrated directly into other software packages. The ability for third party software, such as filtering and monitoring systems, to interact with integrated Generative AI tools is often very limited. It is not clear whether schools are expected to block access to unapproved tools, but it may not be possible for the school to disable integrated Generative AI tools (either through the software itself, or through the school's filtering system). Schools may need to make hard choices about whether to completely discontinue using an application if the vendor does not provide any way for them to disable integrated AI tools. Clearly no amount of filtering or monitoring will prevent unapproved AI tools from being used outside of school to help with homework, and schools are in the difficult position of preventing this behaviour from undermining their policy.
- Engage with parents regarding the school's use of AI tools.[217]

215 Department for Education (England), *Generative artificial intelligence in education*, 12 August 2025, "Using AI safely and effectively: Safety should be the top priority when deciding whether to use generative AI in your education setting", ¶ 7.

216 Department for Education (England), *Generative artificial intelligence in education*, 12 August 2025, "Using AI safely and effectively: Safety should be the top priority when deciding whether to use generative AI in your education setting", ¶ 8.
Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Age ratings", ¶¶ 1 – 2;
UK Safer Internet Centre, *Appropriate Filtering*, 2025, "Generative AI Technologies", ¶ 1;
UK Safer Internet Centre, *Appropriate Monitoring*, 2025, "Generative AI Technologies", ¶ 1.

217 Department for Education (England), *Generative artificial intelligence in education*, 12 August 2025, "Using AI safely and effectively: Safety should be the top priority when deciding whether to use generative AI in your education setting", ¶ 10;
Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI", ¶ 4.

- Personal data should not be submitted to generative AI tools unless strictly necessary, and the products and procedures must comply with data protection legislation and privacy policies.[218]
- Be open and transparent about automated decision making and profiling and that data subjects understand and agree to their personal data is being processed by AI tools. The DfE's *Data protection in schools* guidance and the Information Commissioner's Office's guidance on automated decision making are signposted.[219] Also note that the UK GDPR includes restrictions and safeguards regarding automated decision making.[220]
- Materials created by pupils and teachers are usually copyrighted material, and may not usually be used to train an AI without permission (although there are some statutory exemptions). Schools must therefore be aware of whether the tools they are using may be trained from the materials that they are inputting. Some tools will allow users to opt-out of such training.[221]
  Opinion: as their employer, the school would usually be the copyright holder of materials created by teachers in connection with their work. However, it is likely that students will hold the copyright to their own work, and teachers may well create materials outside of their employment with the school, for which they would hold the copyright.
- Schools should be aware that generative AI tools may produce output that infringes the copyright of others. For example, if the AI tool has been trained on copyrighted work without permission, it may reproduce parts of that work in its output.[222]

218 Department for Education (England), *Generative artificial intelligence in education*, 12 August 2025, "Using AI responsibly: Data privacy", ¶¶ 1 – 2;
Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Data protection and privacy", ¶ 4.

219 Department for Education (England), *Generative artificial intelligence in education*, 12 August 2025, "Using AI responsibly: Data privacy", ¶ 3;
Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Opportunities of generative AI for schools and settings: How generative AI can support education", ¶ 4;
Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Age ratings", ¶ 3;
Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Data protection and privacy", ¶ 2.
See also:
- Department for Education (England), *Data protection in schools*.
- Information Commissioner's Office, *What if we want to profile children or make automated decisions about them?*
- Information Commissioner's Office, *Children's code guidance and resources*.
- Information Commissioner's Office, *Guidance on AI and data protection*.
- South West Grid for Learning, *360 Degree Safe Cymru: School Online Safety Policy Template – Generative Artificial Intelligence (gen AI) in Schools*.

220 UK Government, *United Kingdom General Data Protection Regulation*, Articles 22 – 22D.

221 Department for Education (England), *Generative artificial intelligence in education*, 12 August 2025, "Using AI responsibly: Intellectual property", ¶ 1 – 8.

222 Department for Education (England), *Generative artificial intelligence in education*, 12 August 2025, "Using AI responsibly: Intellectual property: Secondary infringement", ¶ 1 – 8.

Other

- Schools should have a "whole school" approach to online safety, with mechanisms to identify, intervene and escalate concerns.[223]
- Try to engage with parents when setting online safety policies and what systems the schools are using for filtering and monitoring.[224]
- Several links are provided to information about safeguarding when offering remote learning.[225] These make points such as:
    - communicate with parents to suggest turning on their ISP's filters; and
    - 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*.[226] 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.[227]

223 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶¶ 134, 136;
Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.7;
Department of Education (Northern Ireland), *DE Circular 2016/27: Online Safety*, 01 December 2016, ¶ 9.

224 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶¶ 136, 139.

225 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶¶ 139;
Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.8, Annex C.

226 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶¶ 144;
Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, 06 December 2013, ¶ 4.2.
See also:
- Department for Education (England), *Cyber Security Standards for Schools and Colleges*, 2023.

227 Department for Education (England), *Keeping Children Safe in Education*, 2025, ¶¶ 473, 487.

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 guidance refers to things that many schools would have already been doing as a matter of good practice, but many schools still have work to do to change policies, replace older technologies, and restructure their networks, in order to meet the latest expectations. In some cases schools may well find that there is a significant amount of work involved.

One of the main points which is emphasised in each new update of the 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 already met the same challenges.

In particular, the guidance makes it clear that the Designated Safeguarding Lead (DSL) has lead responsibility for safeguarding and online safety, yet communication between a school and their filtering provider is frequently only through the school's IT support. We often feel that schools would be in a much better position to achieve their safeguarding objectives, if the DSL and filtering provider were to directly work together.

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

We will also be continuing our well received series of online safety webinars oving the coming year. If you are interested in attending one, please contact webinar@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 A: Wales

What's Changed?

The Welsh Government has published new, much more comprehensive online safety guidance this year. Requirements that already applied to Wales, which have been reiterated by the new guidance are not listed in this updates section (i.e. where the new guidance just reiterates requirements that already exist in other Welsh guidance), although they are linked in the appropriate footnotes elsewhere in this document.

Updates to Roles and Responsibilities

- Policies and practices should be developed and agreed with key staff, including the designated safeguarding person, education technology support partner, and the SLT.[228]
- Assigned roles must be identified and allocated, with clear responsibilities and actions to be taken in the event of a safeguarding alert.[229]
- The SLT is responsible for ensuring that all staff understand their role, are appropriately trained, adhere to policies and practices and know what action to take on reports and concerns.[230]
- The SLT is responsible for agreeing a clear review structure (see *Updates to Reviews*, below).[231]

Updates to Teaching

- Schools must educate learners and staff on responsible and considerate online behaviour, and privacy protection. The *keeping safe online* area of *Hwb* is signposted[232]

Updates to Filtering and Monitoring

The Welsh guidance uses the term "online safeguarding solution" in place of "technical monitoring system" that is used by the English guidance. The Welsh guidance frequently conflates filtering and monitoring, often using the term "web filtering" in contexts which clearly refer to monitoring. We have therefore largely assumed that requirements for web filtering also apply to monitoring.

- Filtering and monitoring systems must be supplemented by effective supervision.[233]

228 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC4", ¶ 3.
229 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC4", ¶ 3.
230 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC4", ¶ 4;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC5", ¶ 1.
231 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 3.
232 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC4", ¶¶ 4 – 5;
See also:
- Education Wales (Wales), *Keeping safe online: Online Safety*.

233 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "Overview", ¶ 2;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC4", ¶ 2.

- Every internet request that is transmitted via a school's network should be automatically scanned by a filtering and monitoring system.[234]
- Web traffic should be analysed in real-time, covering multi-lingual text, images and videos.[235]
- Filtering and monitoring should be performed both on-device (where possible), and at the network level.[236]
- There should be comprehensive reporting capabilities to detect both security and policy violations.[237]
- Filtering and monitoring should be applied to all school owned end-user devices and there should be a full web audit trail for safeguarding alerts for school owned devices, both in school and outside of the school network.[238]
- Authenticated access should be used to allow filtering and monitoring systems to distinguish between different users and provide effective and informative safeguarding alerts.[239]
- Age appropriate controls must be applied across all networks, including guest and visitor networks.[240]
- Allow and deny lists can be used to ensure that web filtering does not restrict learning and teaching.[241]
- A web page may contain content belonging to more than one category, and web filtering and monitoring should ensure that content associated with a blocked category is detected.[242]
- The Welsh Government has provided a fairly exhaustive table of categories to be allowed or blocked for each school year group in their *Web filtering category classifications* document, which has been updated this year. Where appropriate, schools should adopt these categories in line with their learners' cognitive understanding rather than strictly by year group.[243]

234 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC1", ¶ 1.
235 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC1", ¶ 2.
236 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC1", ¶ 2.
237 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC1", ¶ 3.
238 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC1", ¶ 3;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC7", ¶ 1.
239 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC2", ¶ 1;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC7", ¶ 3.
240 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC2", ¶ 2;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC3", ¶ 1.
241 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC2", ¶ 2;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC3", ¶ 1.
242 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC3", ¶ 2.
243 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC3", ¶ 3;
See also:
- Education Wales (Wales), *Web filtering category classifications*.

Opinion: This table was developed in collaboration with Smoothwall, and mapping this large list of categories onto another product is not straight forward.

- The head teacher is accountable for deciding which content is blocked or allowed.[244]
- The guidance notes that the Welsh Government offers the "Websafe" solution as part of the PSBA network.
  Opinion: Although the guidance states that Websafe has been accredited in accordance with the UK Safer Internet Centre filtering standards, is should be noted that, at time of writing, the UK Safer Internet Centre's website neither listed Websafe as an accredited product, nor did it provide any self-certification response for the Websafe product.
- Filters and monitoring systems should generate safeguarding alerts or reports when harmful or inappropriate content is detected.[245]
- Additional real-time alerts should be generated where a user may be at risk or has been exposed to inappropriate or harmful content, to enable key staff to provide proactive support.[246]

Updates to Reviews

- Safeguarding alerts should be included in the review process and may inform the need to conduct a review.[247]
- The school's web filtering and online safeguarding policies and processes should be reviewed:[248]
  - at least annually;
  - when a safeguarding risk is identified;
  - when working practices change (e.g. introduction of remote access, BYOD, etc.); and
  - when new technology is introduced.
- The SLT is responsible for agreeing a clear review structure, which ensures that the following are assessed:[249]
  - implementation of related safeguarding and technology policies and procedures;
  - roles and responsibilities (including staff training);
  - monitoring mechanisms and strategies; and

244 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC3", ¶ 3.
245 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC4", ¶ 2;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC5", ¶¶ 1, 3.
246 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC4", ¶ 2;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC5", ¶¶ 1 – 2.
247 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC5", ¶ 3.
248 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 2.
249 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 3.

- any safeguarding alerts or incidents encountered since the previous review.

- Identify a lead to oversee the review, actively seeking feedback from stakeholders such as the DSP, digital lead and practicioners, in order to identify and address areas for enhancement.[250]
- Have a clear process to investigate, implement and clearly communicate actions arising to all relevant parties.[251]
- The review lead is responsible for providing their governing body with assurance that the filtering and monitoring systems are working effectively.[252]

Updates to Checks

- Filtering and monitoring should be continually monitored across a range of different locations and device types to ensure that it remains effective. The SWGfL's testfiltering.com tool is signposted.[253]
  Opinion: although this is a good place to start, this tool only performs a few rudimentary 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. Do not treat the results of testfiltering.com as a simple pass / fail, but instead check whether they match your policy. For example, if testfiltering.com shows that offensive language is not being blocked for staff, this is not a "failure" if your policy is to not block offensive language for staff (we would not recommend blocking offensive language for adults as it is likely to result in over-blocking).

Updates to Generative AI

The Welsh Government has published guidance on the use of generative artificial intelligence within schools. Much of the guidance is non-specific, and also includes information not related to online safety. Only the information that specifically relates to online safety is listed below.

- Ensure that AI tools and services which are used protects individual rights and doesn't prevent schools from meeting their data protection obligations.[254] The Information Commissioner's Office's *Childrens Code*, *AI and Data Protection Risk Toolkit*, and the

250 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 4.
251 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 4.
252 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 5.
253 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 1.
254 Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Opportunities of generative AI for schools and settings: How generative AI can support education", ¶ 4;
Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Age ratings", ¶ 3;
Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Data protection and privacy", ¶ 2.
See also:
- Information Commissioner's Office, *Children's code guidance and resources*.
- Information Commissioner's Office, *Guidance on AI and data protection*.
- South West Grid for Learning, *360 safe Cymru: School Online Safety Policy Template – Generative Artificial Intelligence (gen AI) in Schools*.

South West Grid for Learning's *360 Degrees Safe Cymru generative AI policy template* are all signposted.

- Schools should seek advice from their Data Protection Officer and undertake a data protection impact assessment (DPIA).[255]
- Engage with parents and carers regarding schools' use of generative AI.[256]
- Consider the age ratings of generative AI tools and the safety concerns.[257]
- Schools should be aware of the risk of biases, both overt and subtle, within AI tools, as well as the risk of them generating harmful content, such as that which promotes violence, hate or misinformation.[258]
- Encourage learners and staff to report any concerning content generated by AI tools to the provider, and if not satisfactorily resolved they should escalate their concerns to the relevant regulator.[259]
- Confidential or sensitive information, or personal data, must never be entered into a generative AI tool.[260] This requirement is somewhat stronger than the English guidance, which allows for personal data to be submitted where "*strictly necessary*".

Other Updates

- The Education Wales *Device Management Standards* document is signposted with respect to managing school owned devices which are being provided to end-users for use outside of the school network.[261]
- If the school loans a device to a learner to be used outside of the school network, appropriate acceptable use conditions should be agreed with parents and carers, which make it clear that the parent or carer is responsible for monitoring the learner's online activities at home.[262]
- If a school "gifts" a device to a learner or family, it is important to make clear that the school is no longer responsible for management or ownership of the device.[263]

255 Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI", ¶ 3.
256 Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI", ¶ 4.
257 Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Age ratings", ¶¶ 1 – 2.
258 Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Bias, discrimination, stereotyping and harmful content", ¶ 2.
259 Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Bias, discrimination, stereotyping and harmful content", ¶ 4.
260 Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Data protection and privacy", ¶ 4.
261 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC7", ¶ 2;
See also:
- Education Wales (Wales), *Device Management Standards*.
262 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC7", ¶ 4.
263 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC7", ¶ 5.

- A number of requirements have been placed specifically on iOS devices:
  - Apple iOS devices must be enrolled and managed with a mobile device management (MDM) solution.[264]
  - A safeguarding app should be used on Apple iOS devices in place of standard web browsers.[265]
    Opinion: Whilst Apple devices do have certain privacy-enhancing functions, a properly configured network level web filter should be able to monitor and filter the traffic as they normally would. However, on-device filtering and monitoring solutions may be unable to monitor and filter a standard web browser.
  - Assess the configuration options available in Apple Managed App Configuration to enforce settings and policies.[266]
  - Use an MDM solution to distribute apps.[267]
  - Achieve a balance between the school's security and safeguarding considerations and the user's ability to personalise the device.[268]
  - Where devices are used by multiple users and individual users cannot be identified through authentication, implement additional safeguarding controls, such as increased staff supervision.[269]
  - Care should be taken when assessing the apps which are allowed on school devices, as a monitoring system cannot monitor iOS apps. Evaluate:[270]
    - whether the app opens links in a web browser, and if so whether it will use the default browser and therefore be filtered;
    - whether the app contains an embedded web browser that may not be subject to filtering or monitoring;
    - whether the app permits access to other content which may need to be controlled, such as videos or chat. If so, does the app have its own additional controls?; and
    - can the app be accessed through a web browser instead of installing a stand-alone app? If so, it may be subject to the school's standard filtering and monitoring.

264 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶ 1.
265 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶ 5.
266 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶ 6.
267 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶ 6.
268 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶ 6.
269 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶ 7.
270 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶¶ 8 – 10.

Key Differences Compared to England

The guidance for Wales is nowhere near 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.

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.[271]
- 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.[272]
- 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.[273]
- The SLT is responsible for agreeing a clear review structure (see *Reviews*, below).[274]

Training

- The staff training requirements are largely the same as in England, but the guidance refers to safeguarding in general, rather than *online* safety. However, the DSP should have online safety training specifically.[275]
- The DSP should provide an annual briefing and regular updates at staff meetings.[276]

Teaching

- Whereas the English guidance discusses teaching students, the Welsh guidance includes a requirement for schools to educate both learners and staff on responsible and considerate online behaviour, and privacy protection. The *keeping safe online* area of *Hwb* is signposted.[277]

271 Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶¶ 2.14 - 2.15.
272 Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶ 2.16.
273 Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶ 2.9.
274 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 3.
275 Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶ 2.14.
276 Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶ 3.60.
277 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC4", ¶¶ 4 – 5; See also: Education Wales (Wales), Keeping safe online: Online Safety.

Filtering and Monitoring

The Welsh guidance uses the term "online safeguarding solution" in place of "technical monitoring system" that is used by the English guidance. The Welsh guidance frequently conflates filtering and monitoring, often using the term "web filtering" in contexts which clearly refer to monitoring. We have therefore largely assumed that requirements for web filtering also apply to monitoring.

- The statutory guidance refers to the *Education Digital Standards Web filtering* document,[278] which has now been replaced by the, more comprehensive, web filtering and online safeguarding guidance. The UK Safer Internet Centre's guidance is not signposted.
- Every internet request that is transmitted via a school's network should be automatically scanned by a filtering and monitoring system.[279]
- Web traffic should be analysed in real-time, covering multi-lingual text, images and videos.[280]
- Filtering and monitoring should be performed both on-device (where possible), and at the network level.[281]
- There should be comprehensive reporting capabilities to detect both security and policy violations.[282]
- The English guidance expects remote devices to be filtered, but is rather more vague when it comes to monitoring, whereas the Welsh guidance specifically refers to there being a full web audit trail for safeguarding alerts for school owned devices, both in school and outside of the school network, making it clear that these devices should be both filtered and monitored.[283]
- Authenticated access should be used to allow filtering and monitoring systems to distinguish between different users and provide effective and informative safeguarding alerts.[284] The English guidance only *implies* that authenticated access should be used in the context of filtering, whereas the Welsh guidance is explicit that it should be used for both filtering and monitoring.
- Allow and deny lists can be used to ensure that web filtering does not restrict learning and teaching.[285]

278 Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶ 7.7;
See also:
- Education Wales (Wales): *Web filtering*.

279 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC1", ¶ 1.
280 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC1", ¶ 2.
281 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC1", ¶ 2.
282 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC1", ¶ 3.
283 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC1", ¶ 3;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC7", ¶ 1.
284 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC2", ¶ 1;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC7", ¶ 3.
285 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC2", ¶ 2;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC3", ¶ 1.

- A web page may contain content belonging to more than one category, and web filtering and monitoring should ensure that content associated with a blocked category is detected.[286]
- The Welsh Government has provided a fairly exhaustive table of categories to be allowed or blocked for each school year group in their Web filtering category classifications document, which has been updated this year. Where appropriate, schools should adopt these categories in line with their learners' cognitive understanding rather than strictly by year group.[287]
  Opinion: This table was developed in collaboration with Smoothwall, and mapping this large list of categories onto another product is not straight forward.
- The head teacher is accountable for deciding which content is blocked or allowed.[288]
- The guidance notes that the Welsh Government offers the "Websafe" solution as part of the PSBA network.
  Opinion: Although the guidance states that Websafe has been accredited in accordance with the UK Safer Internet Centre filtering standards, is should be noted that, at time of writing, the UK Safer Internet Centre's website neither listed Websafe as an accredited product, nor did it provide any self-certification response for the Websafe product.
- Additional real-time alerts should be generated where a user may be at risk or has been exposed to inappropriate or harmful content, to enable key staff to provide proactive support.[289]

Reviews

- Safeguarding alerts should be included in the review process and may inform the need to conduct a review.[290]
- The SLT is responsible for agreeing a clear review structure, which ensures that the following are assessed:[291]
  - implementation of related safeguarding and technology policies and procedures;
  - roles and responsibilities (including staff training);
  - monitoring mechanisms and strategies; and
  - any safeguarding alerts or incidents encountered since the previous review.

286 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC3", ¶ 2.
287 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC3", ¶ 3;
See also:
- Education Wales (Wales), *Web filtering category classifications*.

288 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC3", ¶ 3.
289 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC4", ¶ 2;
Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC5", ¶¶ 1 – 2.
290 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC5", ¶ 3.
291 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 3.

- Identify a lead to oversee the review, actively seeking feedback from stakeholders such as the DSP, digital lead and practitioners, in order to identify and address areas for enhancement.[292]
- Have a clear process to investigate, implement and clearly communicate actions arising to all relevant parties.[293]
- The review lead is responsible for providing their governing body with assurance that the filtering and monitoring systems are working effectively.[294]

Mobile Phones

Wales currently has no specific guidance regarding the use of smart phones within schools. However, the Senedd plans to produce guidance which restricts their use.[295]

Generative AI

The Welsh Government has published guidance on the use of generative artificial intelligence within schools. Much of the guidance is non-specific, and also includes information not related to online safety. Only the information that specifically relates to online safety is listed below.

- Ensure that AI tools and services which are used protect individual rights and don't prevent schools from meeting their data protection obligations.[296] The Information Commissioner's Office's *Childrens Code*, *AI and Data Protection Risk Toolkit*, and the South West Grid for Learning's *360 Degree Safe Cymru generative AI policy* template are all signposted.
- Schools should seek advice from their Data Protection Officer and undertake a data protection impact assessment (DPIA).[297]
- Schools should be aware of the risk of biases, both overt and subtle, within AI tools, as well as the risk of them generating harmful content, such as that which promotes violence, hate or misinformation.[298]

---

292 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 4.
293 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 4.
294 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC6", ¶ 5.
295 Welsh Government (Wales), *Petition response to P-06-1482: Ban smartphones in all schools in Wales*, 16 April 2025;
Welsh Government (Wales), *Plenary*, 14 May 2025, § 6.
296 Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Opportunities of generative AI for schools and settings: How generative AI can support education", ¶ 4;
Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Age ratings", ¶ 3;
Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Data protection and privacy", ¶ 2.
See also:
- Information Commissioner's Office, *Children's code guidance and resources*.
- Information Commissioner's Office, *Guidance on AI and data protection*.
- South West Grid for Learning, *360 safe Cymru: School Online Safety Policy Template – Generative Artificial Intelligence (gen AI) in Schools*.

297 Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI", ¶ 3.
298 Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Bias, discrimination, stereotyping and harmful content", ¶ 2.

- Encourage learners and staff to report any concerning content generated by AI tools to the provider, and if not satisfactorily resolved they should escalate their concerns to the relevant regulator.[299]
- Confidential or sensitive information, or personal data, must never be entered into a generative AI tool.[300] This requirement is somewhat stronger than the English guidance, which allows for personal data to be submitted where "*strictly necessary*".

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.[301]
- Estyn inspections should verify schools' ability to recognise, respond to and resolve online safety issues.[302]
- The Education Wales *Device Management Standards* document is signposted with respect to managing school owned devices which are being provided to end-users for use outside of the school network.[303]
- If the school loans a device to a learner to be used outside of the school network, appropriate acceptable use conditions should be agreed with parents and carers, which make it clear that the parent or carer is responsible for monitoring the learner's online activities at home.[304]
- If a school "gifts" a device to a learner or family, it is important to make clear that the school is no longer responsible for management or ownership of the device.[305]
- A number of requirements have been placed specifically on iOS devices:
    - Apple iOS devices must be enrolled and managed with a mobile device management (MDM) solution.[306]
    - A safeguarding app should be used on Apple iOS devices in place of standard web browsers.[307]
      Opinion: Whilst Apple devices do have certain privacy-enhancing functions, a properly configured network level web filter should be able to monitor and filter the traffic as they

299 Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Bias, discrimination, stereotyping and harmful content", ¶ 4.
300 Education Wales (Wales), *Generative artificial intelligence in education*, 2025, "Considerations for schools and settings around generative AI: Data protection and privacy", ¶ 4.
301 Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶¶ 2.8, 2.26, 4.23.
302 Education Wales (Wales), *Keeping Learners Safe, 2022,* ¶ 7.16.
303 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC7", ¶ 2;
See also:
- Education Wales (Wales), *Device Management Standards*.

304 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC7", ¶ 4.
305 Education Wales (Wales), *Web filtering and online safeguarding*, 07 February 2025, "AC7", ¶ 5.
306 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶ 1.
307 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶ 5.

normally would. However, on-device filtering and monitoring solutions may be unable to monitor and filter a standard web browser.

- Assess the configuration options available in Apple Managed App Configuration to enforce settings and policies.[308]
- Achieve a balance between the school's security and safeguarding considerations and the user's ability to personalise the device.[309]
- Where devices are used by multiple users and cannot be authenticated, implement additional safeguarding controls, such as increased staff supervision.[310]
- Care should be taken when assessing the apps which are allowed on school devices, as a monitoring system cannot monitor iOS apps. Evaluate:[311]
  - whether the app opens links in a web browser, and if so whether it will use the default browser and therefore be filtered;
  - whether the app contains an embedded web browser that may not be subject to filtering or monitoring;
  - whether the app permits access to other content which may need to be controlled, such as videos or chat. If so, does the app have its own additional controls?; and
  - can the app be accessed through a web browser instead of installing a stand-alone app? If so, it may be subject to the school's standard filtering and monitoring.

Appendix B: Scotland

What's Changed?

There have been no updates to the online safety guidance for Scotland this year.

Key Differences Compared to England

The guidance for Scotland is nowhere near 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.

308 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶ 6.
309 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶ 6.
310 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶ 7.
311 Education Wales (Wales), *Web filtering considerations for Apple iOS devices*, 11 September 2025, "Additional considerations when using Apple iOS devices", ¶¶ 8 – 10.

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*.[312]

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.*"[313]

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.[314]

There is also information about online safety, including education about online safety, in *The National Guidance for Child Protection In Scotland.*[315] However, it makes no mention of filtering and monitoring.

Mobile Phones

The Scottish Government has published *Mobile phones: guidance for Scotland's schools*[316], which provides some very limited guidance regarding the use of mobile phones at school.

Rather than restricting mobile phones in schools, as England and Northern Ireland have done (and soon Wales), the Scottish Government has left the decision up to head teachers.[317]

Schools should develop a policy for the use of mobile phones within school, which includes:[318]

- Digital etiquette (standards of conduct when using mobile phones):
    - Restrictions or limitations on personal mobile phone use within school grounds within the school day, at social school events and on school outings.[319]
    - The prohibition of mobile phones during exams, unless used as part of an agreed reasonable adjustment, with a clear consequence of no award.[320]
    - Guidelines for both staff, pupils, parents and carers and visitors to the school, on the need to respect privacy, particularly with respect to photographs and filming.[321] In

312 Scottish Government (Scotland), Internet Safety for Children and Young People, 2017.
313 Scottish Government (Scotland), *Internet Safety for Children and Young People*, 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".
314 Scottish Government (Scotland), *Internet Safety for Children and Young People*, 2017, Annex D, "Regulation and Guidance".
315 Scottish Government (Scotland), *National Guidance for Child Protection in Scotland*, 2023.
316 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024.
317 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, "Foreword", ¶¶ 3 – 5.
318 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, ¶ 14.
319 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, ¶ 15.
320 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, ¶ 16.
321 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, ¶ 17.

particular, the uploading of images and recordings should not be uploaded to social media without express permission of the subjects.[322]

- Policy on procedures for restriction, safe storage and the return of mobile phones.[323]
- Consideration of situations where mobile phones may be used by pupils with particular needs.[324]
- Consistent application of policy.[325]
- Clearly stated responsibility for loss, theft or breakage of personal mobile phones.[326]

- Digital rights and responsibilities (what individuals can and cannot do):[327]
  - Agreed consequences for the misuse of mobile phones.
  - Clear procedures for the removal and return of mobile phones as a result of inappropriate use.
  - Clear protocols for reporting misuse, and support available for staff and students who have been harassed.
  - An expectation that staff will respond consistently.
- Safe and secure use of mobile technology (precautions that can be taken to ensure digital safety).[328]

Pupils, staff, parents, carers and the wider school community should be consulted with regards to any restrictions.[329]

Appendix C: Northern Ireland

What's Changed?

There have been no updates to the online safety guidance for Northern Ireland this year.

Key Differences Compared to England

The guidance for Northern Ireland is nowhere near 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.

322 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, ¶ 18.
323 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, ¶ 18.
324 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, ¶ 18.
325 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, ¶ 18.
326 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, ¶ 18.
327 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, ¶ 21.
328 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, ¶ 22 – 23.
329 Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 15 August 2024, ¶ 19.

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.[330]
- 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.).[331]
- One or more designated members of staff should have a higher level of expertise around online safety.[332]

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.[333] 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.*"[334]
- Governors' safeguarding training should be refreshed every 4 years.[335]
- DTs and DDTs should attend a two day "*CPSS Introduction to Child Protection*" course and a refresher every 3 years[336].

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 devices, is well prepared and planned, it can benefit learning and teaching inside and beyond the classroom.*"[337]

330 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, §§ 3, 4.1, 4.2.4, 4.2.5, 4.3, Annex A.
331 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 4.2.
332 Department of Education (Northern Ireland), *DE Circular 2016/27: Online Safety*, 01 December 2016, ¶ 9.
333 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 4.1.
334 Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, 06 December 2013, ¶ 4.1.i.
335 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 4.1.
336 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 4.7.2.
337 Department of Education (Northern Ireland), *DE Circular 2016/26: Effective Educational Uses of Mobile Digital Devices*, 01 December 2016, ¶ 2.

Filtering and Monitoring

- Northern Irish schools are also required to have filtering and monitoring,[338] 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.[339]

Reviews

- The child protection policy should be reviewed annually, but the guidance does not mention *online* safety.[340]
- The anti-bullying policy should be reviewed every 4 years, and should integrate the online safety policy.[341]
- 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.[342]

Mobile Phones

- Whereas the English guidance states that the mobile phone policy should be part of the school's behaviour policy, schools in Northern Ireland have the option of writing a stand alone document instead.[343]

Other

- Schools should have a child protection policy, which should reference the online safety policy.[344]
- Governors should receive an annual report on all child protection matters, but the guidance does not mention *online* safety.[345]
- All policies, including the online safety policy, should be issued to parents at intake and it is advisable to keep parents informed thereafter.[346]

338 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.8;
Department of Education (Northern Ireland), *DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools*, 16 July 2007, ¶ 2.ii;
Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, 06 December 2013, ¶ 4.2.
339 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.8;
Department of Education (Northern Ireland), *DE Circular 2011/22: Internet Safety*, 27 September 2011, ¶¶ 2, 5, 8, Annex 2.ii, Annex2.viii.
340 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, §§ 4.1, 4.3.1.
341 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, §§ 4.1, 6.7.
342 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, §§ 4.1 - 4.2, 6.7.
343 Department of Education (Northern Ireland), *DE Circular 2024/14: Guidance for Schools on Pupils' Personal Use of Mobile Phones and other Similar Devices During the School Day*, 03 September 2024, ¶¶ 4, 18, 21 – 22.
344 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, §§ 3, 4.1, 4.3, Annex A.
345 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 4.1.
346 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 4.9;
Department of Education (Northern Ireland), *DE Circular 2011/22: Internet Safety*, 27 September 2011, ¶ 11.

- 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.[347]
- Engage with parents to share information, advice and guidance on the appropriate and safe use of technology.[348]
- The guidance provides advice regarding sexting[349].
- Maintain a record of potential breaches of online safety in an Online Safety Risk Register[350].

347 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.7.
348 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.8;
Department of Education (Northern Ireland), *DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools*, 16 July 2007, ¶ 2.iii;
Department of Education (Northern Ireland), *DE Circular 2016/27: Online Safety*, 01 December 2016, ¶¶ 9, 17.
349 Department of Education (Northern Ireland), *Safeguarding and Child Protection in Schools*, 2022, § 6.9.
350 Department of Education (Northern Ireland), *DE Circular 2016/27: Online Safety*, 01 December 2016, ¶¶ 9, 17.

Bibliography

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

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.

Department for Education (England), Data protection in schools, https://www.gov.uk/guidance/data-protection-in-schools/what-data-protection-means-for-schools.

Department for Education (England), *Filtering and Monitoring Standards for Schools and Colleges*, 2025, https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges.

Department for Education (England), *Generative AI: Product safety expectations*, https://www.gov.uk/government/publications/generative-ai-product-safety-expectations/generative-ai-product-safety-expectations.

Department for Education (England), *Generative artificial intelligence in education*, 2025, https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education#safety-should-be-the-top-priority-when-deciding-whether-to-use-generative-ai-in-your-education-setting.

Department for Education (England), *Keeping Children Safe in Education*, 2025, https://assets.publishing.service.gov.uk/media/68add931969253904d155860/Keeping_children_safe_in_education_from_1_September_2025.pdf.

Department for Education (England), *Mobile phones in schools*, February 2024, https://assets.publishing.service.gov.uk/media/65cf5f2a4239310011b7b916/Mobile_phones_in_schools_guidance.pdf.

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.

Department for Education (England), *Plan Technology for your School*, https://www.gov.uk/guidance/plan-technology-for-your-school.

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

Department of Education (Northern Ireland), *DE Circular 2007/01: Acceptable use of the Internet and Digital Technologies in Schools*, 16 July 2007,

https://www.education-ni.gov.uk/publications/circular-200701-acceptable-use-internet-schools.

Department of Education (Northern Ireland), *DE Circular 2011/22: Internet Safety,* 27 September 2011, https://www.education-ni.gov.uk/publications/circular-201122-internet-safety.

Department of Education (Northern Ireland), *DE Circular 2013/25: eSafety Guidance*, 06 December 2013, https://www.education-ni.gov.uk/publications/circular-201325-esafety-guidance.

Department of Education (Northern Ireland), *DE Circular 2016/26: Effective Educational Uses of Mobile Digital Devices*, 01 December 2016, https://www.education-ni.gov.uk/publications/circular-201626-effective-educational-uses-mobile-digital-devices.

Department of Education (Northern Ireland), *DE Circular 2016/27: Online Safety*, 01 December 2016, https://www.education-ni.gov.uk/publications/circular-201627-online-safety.

Department of Education (Northern Ireland), *DE Circular 2024/14: Guidance for Schools on Pupils' Personal Use of Mobile Phones and other Similar Devices During the School Day*, 03 September 2024, https://www.education-ni.gov.uk/publications/circular-202414-guidance-schools-pupils-personal-use-mobile-phones-and-other-similar-devices-during.

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

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.

Education Wales (Wales), *Education Digital Standards: Device Management Standards*, https://hwb.gov.wales/school-improvement-and-leadership/education-digital-standards/device-management-standards/.

Education Wales (Wales), *Education Digital Standards: Generative artificial intelligence in education*, 2025, https://hwb.gov.wales/school-improvement-and-leadership/education-digital-standards/generative-artificial-intelligence-in-education.

Education Wales (Wales), *Education Digital Standards: Web filtering and online safeguarding*, 07 February 2025, https://hwb.gov.wales/education-digital-standards/web-filtering-and-online-safeguarding.

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

Education Wales (Wales), *Keeping safe online*: Online Safety, https://hwb.gov.wales/keeping-safe-online/online-safety/.

Education Wales (Wales), *Web filtering category classifications*, https://hwb.gov.wales/api/storage/6d15f714-37bb-46f9-9e7a-82acf4d79175/250310-web-filtering-category-classifications.pdf.

Education Wales (Wales), *Education Digital Standards: Web filtering considerations for Apple iOS devices*, 11 September 2025, https://hwb.gov.wales/school-improvement-and-leadership/education-digital-standards/web-filtering-considerations-for-apple-ios-devices/.

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

Independent Schools Inspectorate, *Handbook for the inspection of associated independent schools, including residential (boarding) schools and registered early years settings*, 2024, https://www.isi.net/site/uploads/ISI%20Inspection%20Handbook%20Dec%2024%20MASTER_241209.pdf.

Information Commisioner's Office, *Childrens code guidance and resources*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/.

Information Commissioner's Office, *Guidance on AI and data protection*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/about-this-guidance/.

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/.

Information Commissioner's Office, *What if we want to profile children or make automated decisions about them?*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-if-we-want-to-profile-children-or-make-automated-decisions-about-them/.

London Grid for Learning, *Online Safety Audit*, https://lgfl.net/TypesOfHarm/OnlineSafetyAudit.

Ofsted (England), *School Inspection Handbook*, 2022, https://www.gov.uk/government/publications/school-inspection-handbook-eif/school-inspection-handbook.

Ofsted (England), *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*, https://docs.opendium.com/wiki/Appropriate_Filtering_for_Education_Settings.

Opendium, *UK Online Safety Guidance in 2023*, https://www.opendium.com/blogs/uk-online-safety-guidance-2023.

UK Government, *Online Safety Act 2023*, https://www.legislation.gov.uk/ukpga/2023/50.

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

UK Safer Internet Centre, *Appropriate Filtering for Education Settings*, 2025, https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering.

UK Safer Internet Centre, *Appropriate Monitoring for Schools*, 2025, https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring.

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

UK Safer Internet Centre, *Summary of Substantive Changes*, 2025, https://d1xsi6mgo67kia.cloudfront.net/uploads/2025/05/UKSIC-2025-Substantive-changes.pdf.

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/.

Scottish Government (Scotland), *Mobile phones: guidance for Scotland's schools*, 14 August 2024, https://www.gov.scot/publications/mobile-phone-guidance-scotlands-schools/.

Scottish Government, *National Guidance for Child Protection in Scotland*, 2023, https://www.gov.scot/publications/national-guidance-child-protection-scotland-2021-updated-2023/.

South West Grid for Learning, *360 Degree Safe*, https://360safe.org.uk/.

South West Grid for Learning (Wales), 3*60 Degree Safe Cymru: School Online Safety Policy Template – Generative Artificial Intelligence (gen AI) in schools*, https://hwb.gov.wales/api/storage/ea4707a3-db9b-4a69-9bfe-da38e8c24aae/c5-gen-ai-school-policy-template.docx.

Welsh Government (Wales), Petition response to P-06-1482: Ban smartphones in all schools in Wales, 16 April 2025, https://laiddocuments.senedd.wales/gen-ld17159-en.pdf.

Welsh Government (Wales), Plenary, 14 May 2025, § 6, https://record.assembly.wales/Plenary/15107#C677331.