**Useful links and resources 2025**

**Department for Education**

**1.Keeping Children Safe in Education 2025 (DfE)**

**https://www.gov.uk/government/publications/keeping-children-safe-in-education--2**

**Summary:**

This guidance applies to all schools and colleges and is for headteachers, teachers, staff, governing bodies, proprietors and management committees. It sets out the legal duties you must follow to safeguard and promote the welfare of children and young people under the age of 18 in schools and colleges.

All school and college staff should read Part one of this guidance. Statutory guidance sets out what schools must do to comply with the law. Where the guidance states schools and colleges should do something, you should follow this unless you have a good reason not to.

The 2024 version of the guidance is currently in force. The 2025 version will come into force on 1st September 2025.

**2.Meeting digital and technology standards in schools and colleges (DfE)**

**https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges**

**Summary:**

This is the filtering and monitoring standards for schools and colleges. It sets out what standards your school or college should meet on filtering and monitoring.

**3.Broadband internet standards for schools and colleges (DfE)**

**https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/broadband-internet-standards-for-schools-and-colleges**

**Summary:**

This is the broadband internet standards for schools and colleges. It sets out what standards your school or college should meet on connection type, connection speed, resilience and safeguarding.

**4.Cyber security standards for schools and colleges (DfE)**

**https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/cyber-security-standards-for-schools-and-colleges**

**Summary:**

This is the cyber security standards for schools and colleges. It sets out what standards your school or college should meet on cyber security, user accounts and data protection.

**5.Data protection policies and procedures (DfE)**

**https://www.gov.uk/guidance/data-protection-in-schools/data-protection-policies-and-procedures**

**Summary:**

This guidance shares what you need to do to comply and document compliance with UK GDPR and the Data Protection Act 2018. Under UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA), schools must:

* **comply with the legislation**
* **demonstrate that they’re complying**

You can read more about the personal data you need to document and how to do so on the Information Commissioner’s Office (ICO) website.

**Home Office**

**1.The Prevent duty: safeguarding learners vulnerable to radicalisation (Home Office)**

**https://www.gov.uk/government/publications/the-prevent-duty-safeguarding-learners-vulnerable-to-radicalisation**

**Summary:**

This guidance is designed to explain the Prevent referral process and the statutory responsibilities to keep children, young people and adult learners safe from the risk of extremist ideology or radicalisation. It prepares DSLs to respond effectively and get support for people who may be being exploited by radicalising influences.

**London Grid for Learning (LGfL)**

**1.Online Safety Audit (LGfL)**

**https://national.lgfl.net/digisafe/onlinesafetyaudit**

**Summary:**

According to KCSIE “Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face.” This document is designed to help schools complete such an assessment. It is vital that an online safety audit is neither treated as a tick box exercise, nor viewed as a static report: it should be a living document that reflects the fluid realities of technological change, evolving harms and user behaviours. This means for example, the latest national, local and school trends and incidents that will be reflected in your training and policies (see the LGfL template [OS policy](https://safepolicies.lgfl.net/) for national trends they have identified over the past year).

This audit has been broken down into two broad sections:

* **Curriculum, General Approach & Communication**
* **Safe School Systems (technology for safeguarding and safeguarding for technology)**

Remember to share results with your school governors or trustees, to help them fulfil their oversight duties.

**South West Grid for Learning (SWGfL)**

**1.Online Safety Review (360Safe) (SWGfL)**

**https://360safe.org.uk/**

**Summary:**

The tool provides, information that can influence the production or review of online safety policies and develop good practice. A process for identifying strengths and areas for development, opportunities for commitment and involvement from the whole school and a continuum for schools to discuss how they might move from a basic level of provision for online safety to practice that is aspirational and innovative.

**National Cyber Security Centre**

**1.Cyber security training for school staff**

**https://www.ncsc.gov.uk/information/cyber-security-training-schools**

**Summary:**

The NCSC has produced free cyber security training to raise awareness and help school staff manage some of the key cyber threats facing schools. The training is available in two formats:

* **a scripted presentation pack**

for group delivery can be found in the 'Downloads' section of this webpage. The presentation pack can be used by schools and the education sector to help teach school staff at physical or virtual group sessions - like INSET days or staff meetings.

* **a self-learn video**

for staff to complete by themselves is also available on YouTube. The self-learn video includes the same content as the presentation pack but can be undertaken by a member of staff by themselves at a convenient time.

Once you have completed the training you can download a certificate to print to demonstrate that the training has been completed.

* If you watch the training on YouTube, the link to the certificate can be found in the Description field.
* If you watch the training via the embedded view on this page, you can download the certificate.
* If you download the PowerPoint version of the training, also available in the Downloads section, the link can be found on the final slide.

**UK Safer Internet Centre**

**1. Appropriate filtering and monitoring definitions published (UK Safer Internet Centre)**

**https://saferinternet.org.uk/blog/2023-appropriate-filtering-and-monitoring-definitions-published**

**Summary:**

The UK Safer Internet Centre (UKSIC) has published its ‘appropriate’ filtering and monitoring definitions. The definitions help both schools and providers understand what is considered ‘appropriate’.

**2.Test Your Internet Filter (UKSIC / SWGfL)**

**http://testfiltering.com/**

**Summary:**

Test your internet filter to see whether it blocks child abuse and terrorist content.

**3.Filtering provider responses - self-certified by service providers (UKSIC)**

**https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/filtering-provider-responses**

**Summary:**

UKSIC invite filtering providers to self-certify filtering systems using their checklist and their responses are hosted here.

**4.A Guide for education settings and filtering providers (UKCIS)**

**https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring**

**Summary:**

The aim of the documents provided on this website are to help schools and providers comprehend, in conjunction with their completed risk assessment, what should be considered as ‘appropriate’ filtering and monitoring.

**5.Establishing appropriate levels of filtering (UKSIC)**

**https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering**

**Summary:**

The aim of the document is to help education settings (including Early years, schools and FE) and filtering providers comprehend what should be considered as ‘appropriate filtering’. It is important to recognise that no filtering systems can be 100% effective and need to be supported with good teaching and learning practice and effective supervision. As such, filtering systems should be recognised as one of the tools used to support and inform the broader safeguarding provision in settings.

**6.Online safety in schools and colleges: questions from the governing board (UKCIS)**

**https://www.gov.uk/government/publications/online-safety-in-schools-and-colleges-questions-from-the-governing-board**

**Summary:**

Guidance for school governors and trustees to help them support school leaders to keep children safe online. Set out as a list of questions, it includes examples of good and outstanding practice, as well as identifying when governors should be concerned. These questions cover:

* **policies**
* **supporting and reporting mechanisms**
* **staff training**
* **teaching and learning**
* **whole-school community engagement and education**

The guidance also includes a proforma to help senior leaders to record evidence of the above.

**Digital Resilience**

**1.HeadStart Online Digital Resilience Tool (HeadStart Kernow)**

**https://www.headstartkernow.org.uk/digital-resilience/**

**Summary:**

The Online Resilience Tool provides a practical way for professionals to assess young people’s online behaviour and help them make decisions about whether that behaviour represents risk of harm. The Tool was developed as part of the Digital work-stream of the HeadStart Kernow programme in partnership with University of Bournemouth and the Professionals Online Safety Helpline. In total around 1000 children and young people in Cornwall were involved in the development process through workshops and discussion groups over a three-year period. The Digital Resilience Tool is available to download for free.