UK Council for Internet Safety

Online safety in schools and colleges: Questions from the Governing Board

Children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage.

The Department for Education's Keeping Children Safe in Education (2019) statutory guidance states that, "Governing bodies and proprietors should ensure that children are taught about safeguarding, including online safety. Schools and colleges should consider this as part of providing a broad and balanced curriculum. This may include covering relevant issues through Relationships Education and Relationships and Sex Education … Personal, Social, Health and Economic (PSHE) education."

1	**Does the school/college have an up to date online safety policy and acceptable use policies in place?** **How does the school/college assess that they are clear, understood and respected by all children and staff?**
Why this question?	The Department for Education's (DfE) 2019 'Keeping Children Safe in Education' (KCSIE) statutory guidance states that "Governing bodies and proprietors should ensure there are appropriate procedures in place…to safeguard and promote children's welfare… this should include … acceptable use of technologies…and communications including the use of social media." Annex C KCSIE also states that 'Governors and proprietors should consider a whole school/college approach to online safety. This will include a clear policy on the use of mobile technology in the school.' The 2019 DfE guidance document 'Teaching online safety in schools' states that schools should create "a culture that incorporates the principles of online safety across all elements of school life. The principles should be reflected in the school's policies and practice where appropriate, and should be communicated with staff, pupils/students and parents. This will include, for example, in the child protection policy clear processes for reporting incidents or concerns."
What to look for?	■ Systematic and regular review of safeguarding policies, including online safety, at least on an annual basis. ■ Evidence that online safety policies are readily available (e.g. school/college website, staff handbooks, posters, etc). ■ Pupils/students, staff and parents are aware of online safety rules and expectations.
What is good practice?	■ Collaborative production and review of policies, for example, evidence of the active use of pupils/students' and parents' views. ■ Evidence of monitoring and evaluation processes to ensure understanding of, and adherence to, online safety policies. ■ Pupils/students, staff and parents are aware of online safety behaviour and expectations, including the acceptable use of technologies and the use of mobile technology. ■ The school/college child protection policy recognises peer on peer abuse concerns which can take place online. ■ Linked to and a part of other policies, such as safeguarding and child protection,

	pupil/student behaviour, staff code of conduct. ■ Policies do not use and, where appropriate, actively challenge 'victim blaming' language and recognise that children are never responsible for the harm which they may experience, especially given the online context / pervasive nature of social media technology
When should you be concerned?	■ No or minimal online safety policies ■ Policy is generic and not specifically relevant to the pupils'/students' needs in the school/college. ■ No/irregular review of online safety policies. ■ Policies exist but are not publicised to the school/college body and/or are not known by staff and pupils/students.
Where to go for more support	■ Kent County Council/The Education People – Acceptable Use Policy templates for education settings https://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety ■ London Grid for Learning (LGfL) – Online Safety Policy and Acceptable Use Templates http://onlinesafety.lgfl.net ■ South West Grid for Learning (SWGfL) - Online Safety Policy Templates http://swgfl.org.uk/products-services/esafety/resources/online-safety-policy-templates ■ SWGfL - 360 degree safe' audit tool: https://360safe.org.uk/

2	**What mechanisms does the school/college have in place to support pupils/students, staff and parents facing online safety issues?**
Why this question?	The 2019 DfE guidance document 'Teaching online safety in schools' states that "It is important to create a safe environment in which pupils/students feel comfortable to say what they feel. If a pupil /student thinks they will get into trouble and/or be judged for talking about something which happened to them online they may be put off reporting it and getting help" and "it is essential all pupils/students are clear what the school's reporting mechanisms are". With regards to monitoring and filtering, the 2019 KCSIE statutory guidance states "As schools and colleges increasingly work online it is essential that children are safeguarded from potentially harmful and inappropriate online material. As such governing bodies and proprietors should ensure appropriate filters and appropriate monitoring systems are in place."
What to look for?	■ Online safety clearly recognised as a safeguarding issue within the roles and responsibilities of all staff in the school/college with overall responsibility held by the Designated Safeguarding Leads (DSL). ■ Whole school/college approach, in which robust reporting channels are well-defined, clearly understood and consistent and known by all school/college staff, pupils/students and parents. ■ Clearly described procedures for responding to different online harms (e.g. Sexting; Upskirting; Online Bullying and Online grooming etc.) ■ Links into other relevant policies and procedures e.g. whistleblowing/managing allegations, complaints etc. ■ Leadership staff are aware of and understand the decisions made by the school/college in respect to implementing 'appropriate filtering and monitoring'. ■ Regular review of monitoring and filtering provisions as part of safeguarding

	responsibilities e.g. evidence of communication between technical staff and DSLs.
What is good practice?	■ Online reporting mechanisms for pupils/students and parents. ■ All staff are aware of sources of support for online safety issues, such as the Professionals Online Safety Helpline, Reporting Harmful Content, CEOP and Internet Watch Foundation. https://www.saferinternet.org.uk/helpline/professionals-online-safety-helpline https://www.saferinternet.org.uk/helpline/report-harmful-content https://www.ceop.police.uk/ceop-reporting/ https://report.iwf.org.uk/en ■ The DSL and deputies have the appropriate skills and are trained to deal with the various risks related to online activity. There may be additional nominated members of staff who support this area with their expertise. ■ All staff should receive appropriate safeguarding and child protection training, including online safety (as set out in KCSIE). ■ Planned and effective peer support strategies, e.g. reporting mechanisms/escalation processes supported by all school/college staff. ■ Auditing of online behaviour and harms which provides base line information from the pupils/students about the levels and types of online issues prevalent in the school/college. ■ Regular evaluation of reporting channels and response procedures. ■ Online safety information/data highlighted within the Head Teacher's report to the Governing board. ■ Appropriate filtering and monitoring decisions are regularly reviewed in line with the school/college's needs and relevant information is clearly communicated to staff, pupils/students and parents.
When should you be concerned?	■ No/inconsistent reporting channels. ■ No recording processes to enable the school /college to identify and monitor concerns. ■ Pupils/students and parents unaware of or lack confidence in reporting channels. ■ Staff are unclear of how to support pupils/students and parents with online safety concerns. ■ Appropriate filtering and monitoring approaches are not in place, and/or there is a lack of understanding of the decisions made with respects to appropriate filtering and monitoring by the leadership team.
Where to go for more support	■ DfE 'Keeping Children Safe in Education 2019' - includes a flowchart on page 13, showing actions to take when there are concerns (offline or online) about a child; https://www.gov.uk/government/publications/keeping-children-safe-in-education--2 ■ DfE 'What to do if you're worried a child is being abused': http://www.gov.uk/government/publications/what-to-do-if-youre-worried-a-child-is-being-abused--2 ■ NCA-CEOP Safety Centre – to report online sexual abuse or concerning online communication http://www.ceop.police.uk ■ UK Council for Internet Safety (UKCIS) 'Sexting in Schools and Colleges' https://www.gov.uk/government/publications/sexting-in-schools-and-colleges ■ UK Safer Internet Centre: Appropriate filtering and monitoring guides for schools and education settings: http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/appropriate-filtering-and-monitoring

	■ UK Safer Internet Centre: Professionals Online Safety Helpline: http://www.saferinternet.org.uk/about/helpline ■ Access your local policies and procedures - some local authorities, local safeguarding partners and/or regional broadband consortia may have specific policies and procedures for responding to some online safety risks

3	**How do you ensure that all staff receive appropriate, relevant and regularly updated online safety training?**
Why this question?	The 2019 KCSIE statutory guidance states that "all staff undergo safeguarding and child protection training (including online safety) at induction" and that "online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach". Annex B of 2019 KCSIE statutory guidance states that DSLs should ensure that 'they are able to understand the unique risks associated with online safety", are "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 that they "can recognise the additional risks that children with SEN and disabilities (SEND) face online". The 2019 DfE guidance document 'Teaching online safety in schools' states that "school staff have access to up to date appropriate training/CPD and resources, so that they are confident in covering the required content in a way that is relevant to their pupils/students' lives."
What to look for?	■ Training which improves staff knowledge of, and expertise in, safe behaviours and appropriate use of technologies. ■ Audit of the training needs of all staff. ■ Online safety training as an integral part of the required, at least annual, safeguarding training for all staff. Online safety training as an integral part of induction for all new staff. ■ Online safety training coordinated by the DSL. ■ Evidence that the DSL (and their deputies) has ensured that their knowledge and skills regarding online safety is robust.
What is good practice?	■ DSL and their deputies have a higher level of training, knowledge and expertise on online safety issues, with clearly defined responsibilities related to online safety provision for the school/college community. ■ Expertise in online safety is developed across a pool of staff, to ensure transfer and sustainability of knowledge and training. ■ Online safety training clearly established within the school/college's wider safeguarding training. ■ Training content updated to reflect current research and advances in technology as well as local policy and procedures. ■ Online safety training is given to all new staff as part of induction.
When should you be concerned?	■ DSL and deputies lack appropriate training and authority in online safety. ■ No recognised individual/group for online safety or they lack appropriate training and authority. ■ No, little or out-of-date training for all staff. ■ There are some staff that have no online safety training. ■ Regular updated training (at least annual) is not undertaken.

	■ Training on online safety does not meet the needs of staff. ■ Training based on outdated resources/materials, or materials which lack accuracy. ■ Lack of clarity on who coordinates staff training.
Where to go for more support	■ Childnet's Professional resources: http://www.childnet.com/teachers-and-professionals ■ NCA-CEOP Ambassador course: https://www.thinkuknow.co.uk/professionals/training/ceop-ambassador-course/ ■ NSPCC and NCA-CEOP - Keeping Children Safe Online. an online introductory safeguarding course for anyone who works with children (2019 version): https://www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/ ■ UK Safer Internet Centre training, advice and resources for teachers and professionals: https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff and Online Safety Briefings: https://www.saferinternet.org.uk/training-events/online-safety-live-free-online-safety-events ■ Access any local support available - some local authorities, local safeguarding partners and/or regional broadband consortia offer online safety training for professionals

4	**Describe how your school/college provides the learning required to educate children and young people to build knowledge, skills and confidence with regard to online safety. This will included learning contained within the statutory (September 2020) Relationships Education, Relationships and Sex Education (RSE) and Health Education, the Computing curriculum, Citizenship and other subjects where relevant.**
Why this question?	In England, from September 2020, Relationships Education will be compulsory for all primary aged pupils and Relationships and Sex Education compulsory for all secondary aged pupils[1]. Health Education will be compulsory for all pupils in state-funded schools[2]. Online safety education is embedded throughout these subjects. Children have a right to education about their rights across both online and offline contexts, as well as how to respect the rights of other online users. Children equally have a right to education which teaches them who to ask for help if things go wrong. The internet does not yet provide a safe and equal space for all children, and so we believe they have a right to be taught how to best navigate potential risks online and to have their own safety strategies recognised and supported. Education alone does not protect children. Children are not responsible for their own abuse online or otherwise even if they do not follow the safety messages /education taught in schools and other settings.
What to look for?	■ Teaching draws from the DfE guidance 'Teaching online safety in schools' (June 2019) ■ Teaching enables children and young people to achieve the learning outcomes described within the UK Council for Internet Safety (UKCIS) framework 'Education for a Connected World' (February 2018)

[1] *School means all schools, whether maintained, non-maintained or independent schools including academies and free schools, non-maintained special schools and alternative provision including pupil referral units*

[2] *Guidance on Health Education does not apply to independent schools, which must meet the Independent School Standards as set out in the Education (Independent School Standards) Regulations 2014. However, they may find the sections on PSHE helpful. It does, however, apply to academies and free schools.*

	■ Planned online safety education programme which is: - Taught across all age groups and progresses as pupils/students grow and develop. - Regular as opposed to a one-off online safety session. - Supports pupils/students in developing strategies for navigating the online world. - Embedded across the curriculum. - Incorporates/makes use of relevant national initiatives and opportunities such as Safer Internet Day and Anti-bullying week. ■ Use of appropriate and up-to-date resources. ■ Resources, including visitors from external providers used appropriately to support and compliment internal provision. ■ Accessible to pupils/students at different ages and abilities, such as pupils/students with Special Educational Needs and Disabilities (SEND), or those with English as an additional language. ■ Pupils/students are able to recall, explain and actively use online safety education. ■ Teachers have access to appropriate training, ensuring expertise and understanding underpins their teaching.
What is good practice?	■ Online safety is embedded throughout the school/college curriculum. This means that the opportunity to develop the knowledge, skills and confidence of pupils/students, on issues related to online safety, are planned into all relevant lessons such as in PSHE education, including Relationships and Sex Education, citizenship and computing. ■ Regular review of the online safety curriculum to ensure its relevance to pupils/students. The school/college uses the Education for a Connected World framework to review and quality assure online safety education.
When should you be concerned?	■ Ad-hoc/one-off sessions on online safety, such as sessions only delivered through assemblies or drop-down days. ■ Content used is inaccurate, irrelevant or out of date and/or inappropriate for the age/ability of the pupil/student. ■ Resources/materials used with pupils/students relies on fear, shock or victim blaming approaches. ■ The programme of study in place is not progressive or sustainable e.g. substantial reliance on external providers/visitors to deliver online safety education and/or is delivered in response to a specific issue. ■ No means to evaluate the effectiveness of provision and assess pupils/students' learning in the area. ■ The school/college is failing to teach the statutory requirements for online safety contained within the Relationships Education, Relationships and Sex Education and Health Education guidance. (September 2020) ■ The school/college has not used the Department for Education's 'Teaching online safety in schools' guidance to review and quality assure the programme of study for Online Safety. ■ The programme of study for online safety is not embedded across the curriculum. It is not taught, or minimally taught in PSHE education including Relationships and Sex Education, Computing and Citizenship and is not part of the curriculum offering for other subjects as appropriate. ■ The school/college is not providing a range of learning opportunities necessary to meet the learning objectives, such as those identified in the UKCIS 'Education for a

	Connected World' framework.
Where to go for more support	■ DfE 'Teaching Online Safety in Schools' guidance https://www.gov.uk/government/publications/teaching-online-safety-in-schools ■ DfE Statutory (September 2020) guidance for Relationships Education, Relationships and Sex Education (RSE) and Health Education https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education ■ Childnet http://www.childnet.com/young-people ■ NCA-CEOP's online safety education programme, Thinkuknow: http://www.thinkuknow.co.uk ■ PSHE Association/NPCC using police in the classroom guidance https://www.pshe-association.org.uk/policing ■ UKCIS 'Education for a Connected World' framework: https://www.gov.uk/government/publications/education-for-a-connected-world ■ UKCIS 'Using External Visitors to Support Online Safety Education: Guidance for Educational Settings' https://www.gov.uk/government/publications/using-external-visitors-to-support-online-safety-education-guidance-for-educational-settings

5	**How does the school/college educate parents and the whole school /college community with online safety?**
Why this question?	The 2019 DfE document 'Teaching online safety in school' states that the school culture should "incorporate the principles of online safety across all elements of school life … reflected in the school's policies and practice … communicated with staff, pupils/students and parents." And "Schools should also ensure they extend support to parents, so they are able to incorporate the same principles of online safety at home."
What to look for?	■ Regular communication, awareness-raising and engagement on online safety issues and reporting routes, such as the school/college website and newsletters. ■ Regular opportunities for engagement with parents on online safety issues such as awareness workshops.
What is good practice?	■ Interactive engagement with parents, with the aim of building skills and confidence to support their children in dealing with online harms, as well as general awareness on online safety issues. ■ Regular and relevant online safety resources and sessions offered to parents. Relevant resources will tackle key online risks and behaviours displayed by pupils/students at different ages in the school/college. ■ Evidence of pupils/students educating parents. ■ Online safety information available in a variety of formats, such as for those with English as an additional language.
When should you be concerned?	■ No/minimal awareness-raising on online safety issues. ■ No online safety engagement with parents. ■ Recurrent concerning online behaviours amongst pupils/students (such as younger pupils playing games aimed towards older adolescents and adults).
	■ Childnet: https://www.childnet.com/teachers-and-professionals/staff-led-online-safety-

Where to go for more support	presentations- ■ NCA-CEOP Thinkuknow: https://www.thinkuknow.co.uk/parents/ ■ Netware by NSPCC and O2: https://www.net-aware.org.uk ■ Parent Info by NCA-CEOP and Parent Zone: http://parentinfo.org ■ Parent Zone: http://parentzone.org.uk/ ■ Share Aware by NSPCC and O2: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware ■ UK Safer Internet Centre: http://www.saferinternet.org.uk/advice-and-resources/parents-and-carers ■ Vodafone Digital Parenting resources: http://www.vodafonedigitalparenting.co.uk

This document has been brought to you by the UKCIS Education Working Group made up of the following organisations: