Online safety in schools and colleges: Questions from the Governing Board (2022)

UK Council for Internet Safety

Who is this for?

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 (DfE's) Keeping Children Safe in Education (2022) statutory guidance states that:

"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."

This guidance has been produced by the UK Council for Internet Safety (UKCIS) Education Working Group, on behalf of UKCIS to help senior leaders fulfil the above statutory requirements.

This guidance was first published in November 2016, and amended in June 2020, in line with changes to Keeping Children Safe in Education 2018.

This version has been amended in line with changes to Keeping Children Safe in Education 2022, and was published in September 2022.

What does this guidance cover?

This guidance outlines the questions senior leaders should consider when monitoring their school or college's provision. A proforma to help you record evidence is included in Annex A.

Contents

Part One: Policies **4**

Part Two: Support and reporting mechanisms **7**

Part three: Staff training **10**

Part four: Teaching and learning **13**

Part five: Whole school community engagement and education **17**

Annex A **19**

Part One: Policies

Question(s) to ask

- **Does the school/college have up to date policies that address online safety, mobile and smart technology, social media and acceptable use of technology in place?**
- **How does the school/college assess that policies are clear, understood and respected by all children and staff?**

Why ask these questions?

The DfE's 2022 'Keeping Children Safe in Education' (KCSIE) statutory guidance states that "Online safety and the school or college's approach to it should be reflected in the child protection policy. Considering the 4Cs (Content, Contact, Conduct and Commerce) will provide the basis of an effective online policy". We advise that schools/colleges should address online safety in their child protection policy however, schools/colleges may also opt to address online safety as part of a standalone document.

Schools/colleges should "have a clear policy on the use of mobile and smart technology" which addresses how mobile and smart technology is managed on their premises.

Schools should have "a staff behaviour policy (sometimes called the code of conduct) which should, amongst other things, include acceptable use of technologies (including the use of mobile devices), staff/pupil relationships and communications including the use of social media".

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 evidence to look for:

- The school/college policies reflect the whole school/college approach to online safety and addresses the breadth of online safety issues, for example, the 4 Cs; Content, Contact, Conduct and Commerce.
- Policies are in line with current national guidance, for example 'Keeping Children Safe in Education' (2022) and 'Early Years Foundation Stage' (2021).
- Systematic and regular review of safeguarding policies, including child protection and/or online safety, on an at least annual basis.

- Policies reflect the individual schools' local context. For example, they reference policies and procedures as set out by the Local Safeguarding Partnership and are appropriate and specific to the age/ability of learners and use of technology by the school/college.
- Evidence that policies are readily available. For example, they are available on the school/college website, in staff handbooks, and on posters.
- The mobile and smart technology policy addresses use of school/college provided technology and personally owned devices on the premises. This should include, for example, tablets, games consoles, mobile/smart phones and wearable technology.
- Pupils/students, staff and parents are aware of the behaviour expectations regarding acceptable use of technology. For example, use of technology in the classroom, remote learning, social media and the use of mobile and smart technology.

What does good practice look like:

- Collaborative production and review of policies. For example, evidence of the active use of pupils/students' and parents' views.
- Policies developed or adapted for different audiences. For example, age/ability appropriate versions.
- Evidence of monitoring and evaluation processes to ensure understanding of, and adherence to policies.
- Pupils/students, staff and parents are aware of and understand the online safety behaviour expectations, including the acceptable use of technologies and the use of mobile and smart technology.
- The school/college child protection policy recognises child on child abuse concerns which can take place online. For example, online sexual harassment, cyberbullying and consensual and non-consensual nude and semi-nude image sharing.
- Policies that address online safety are linked to other existing policies as appropriate. For example, pupil/student behaviour, staff code of conduct/behaviour, use of camera/images and anti-bullying
- Where schools opt to have a standalone online safety policy, it is clearly established as part of the school's safeguarding policies, is developed by the Designated Safeguarding Lead and is linked/cross-referenced with existing policies.

- 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 and the pervasive nature of social media and technology.

When should you be concerned:

- No/minimal online safety policies.
- No/irregular review of online safety policies.
- Policies that address online safety are technical policies and/or are developed without oversight from the Designated Safeguarding Lead.
- Policy is generic and not specifically relevant to the pupils'/students' needs in the school/college. For example a national model policy template is used, but local information has not been included, or a policy is adopted by a group of schools/colleges and not adapted for each individual school's/college's context.
- Policies exist but are not publicised to the school/college body and/or are not known and understood by staff and pupils/students.
- Policies use out-of-terms, reference dated technology and/or perpetuate victim-blaming language and attitudes.

Where to go for more support:

- The Education People – Acceptable Use of Technology Policy, Social Media and Mobile and Smart Technology Policy templates for education settings: www.theeducationpeople.org/our-expertise/safeguarding/template-policies-and-guidance/
- London Grid for Learning (LGfL) – Online Safety Policy and Acceptable Use Templates: https://www.lgfl.net/online-safety/resource-centre?s=24
- South West Grid for Learning (SWGfL) - Online Safety Policy Templates: http://swgfl.org.uk/products-services/esafety/resources/online-safety-policy-templates
- South West Grid for Learning (SWGfL) - 360 degree safe audit tool: https://360safe.org.uk/

Part Two: Support and reporting mechanisms

Question to ask

- **What mechanisms does the school/college have in place to support pupils/students, staff and parents facing online safety issues?**

Why ask 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 2022 KCSIE statutory guidance states "governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to [the above] risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and appropriate monitoring systems in place."

What evidence to look for:

- Online safety is 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 to online safety that protects and educates pupils, students and staff in their use of technology with mechanisms to identify, intervene in, and escalate any concerns where appropriate. This includes robust reporting channels that are well-defined and clearly understood by all school/college staff, pupils/students and parents, and are consistently applied.
- Clearly described procedures for responding to different online harms (such as sharing nude and semi-nude images; exposure to fake news; online bullying; online grooming)
- Links into other relevant policies and procedures. For example, whistleblowing and managing allegations and complaints.
- 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. For example, evidence of communication between technical staff and DSLs.

- Recognition of online safety throughout other policies and procedures.

What does good practice look like:

- Well promoted and easily accessible online reporting mechanisms for pupils/students and parents.
- All staff are aware of helplines and reporting mechanisms for online safety issues that are available to adults and/or children, such as the Professionals Online Safety Helpline, Reporting Harmful Content, CEOP and Internet Watch Foundation.
- 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, including governors and trustees, should receive appropriate safeguarding and child protection training, including online safety (as set out in KCSIE), at induction.
- All staff should receive safeguarding and child protection (including online safety) updates as required and at least annually.
- Planned and effective peer support strategies. For example, reporting mechanisms/escalation processes supported by all school/college staff.
- Auditing of online behaviour and harms which provides baseline 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.
- Leadership staff have established a whole school culture that empowers pupils/students to report online safety issues without the fear of being blamed. Staff demonstrate active listening, build trusted relationships to facilitate communication, and provide non-judgemental support

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 are unaware of or have a 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 governors and leadership team.
- No or minimal online safety policies.

Where to go for more support:

- DfE - Keeping Children Safe in Education 2022 (includes a flowchart on page 21, 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
- NCA-CEOP Safety Centre – to report online sexual abuse or concerning online communication: http://www.ceop.police.uk
- UK Council for Internet Safety (UKCIS) - Sharing nudes and semi-nudes: advice for education settings working with children and young people: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
- UK Safer Internet Centre - Appropriate filtering and monitoring guides for schools and education settings: https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring
- UK Safer Internet Centre - Professionals Online Safety Helpline: https://saferinternet.org.uk/professionals-online-safety-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

Part three: Staff training

Question to ask

- **How do you ensure that all staff receive appropriate, relevant and regularly updated online safety training?**

Why ask this question?

The 2022 KCSIE statutory guidance states that “all staff should receive appropriate safeguarding and child protection training (including online safety) at induction” and that the training should be regularly updated with staff receiving updates “at least annually”. In addition, KCSIE requires that “safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning”.

Annex C of KCSIE outlines the role of the designated safeguarding lead and states that “the DSL should take lead responsibility for safeguarding and child protection (including online safety)” and that given the significant level of responsibility involved, they should be given additional time, funding, training and resources to carry out the role effectively. It also states that the DSL should be “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 [as well as] recognising the additional risks that children with SEND face online.”

Part two of KCSIE also states that all governors and trustees should receive appropriate safeguarding and child protection, including online, training at induction. 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/colleges are effective and support the delivery of a robust whole school approach to safeguarding”. This training should be regularly updated.

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 evidence 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 is included in the safeguarding and child protection training that all governors and trustees should receive at induction.

- That all staff training, including training for governors/trustees, is regularly updated.
- 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 does good practice look like:

- 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.
- DSL is given the additional time, funding, training, resources and support they need to carry out the role effectively.
- Expertise in online safety is developed across a pool of staff, to ensure transfer and sustainability of knowledge and training.
- Online safety training is clearly established within the school/college's wider safeguarding training.
- Training content is regularly 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.
- Governors/trustees access appropriate and updated training which includes online safety.

When should you be concerned:

- DSL and deputies lack appropriate training and authority in online safety.
- DSL and deputies are not given enough time and resources to carry out their role effectively.
- No recognised individual/group for online safety or they lack appropriate training and authority.
- No, little or out-of-date training for all staff. If online training is provided then it is not updated frequently/ever.
- There are some staff that have no online safety training.

- Regularly updated training (at least annual) is not undertaken.
- Training on online safety does not meet the needs of staff and there is no audit of staff needs carried out.
- Training is 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 - Professional resources: http://www.childnet.com/teachers-and-professionals
- NCA-CEOP Education - 'Understanding Online Child Sexual Abuse' course: https://www.thinkuknow.co.uk/professionals/training/
- NSPCC and NCA-CEOP - Keeping Children Safe Online: an online introductory safeguarding course for anyone who works with children (2022 version): https://learning.nspcc.org.uk/training/online-safety
- UK Safer Internet Centre - training, advice and resources for teachers and professionals: https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff
- UK Safer Internet Centre - 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

Part four: Teaching and learning

Question to ask

- **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 include 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 ask this question?

In England, online safety has been embedded since 2020 in Relationships Education (Primary), Relationships and Sex Education (Secondary)[1] and Health Education for all pupils in state-funded schools[2]. For many years before 2020, Computing was the main curriculum home for online safety but there is much more detail in the RSHE curriculum.

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. Equally they need to be taught 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 evidence to look for:

- Evidence that online safety is seen as part of and driven by safeguarding, and therefore a subject with obvious leadership and safeguarding team involvement
- Teaching draws from the DfE guidance 'Teaching online safety in schools' (June 2019) and there are no obvious gaps that are not addressed somewhere within the curriculum

[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.

- 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' (2020)
- Proactive, 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 and beyond the curriculum.
    - Incorporates/makes use of relevant national initiatives and opportunities such as Safer Internet Day and Anti-Bullying Week but does not wait to address these issues until a certain part of the year or a dedicated 'online safety week'.
- Reactive and responsive teaching through lessons, conversations and informal chats that reflect issues in the school. For example, bullying on WhatsApp is addressed immediately and not left until a scheduled date where it was planned to be covered in a lesson.
- Appropriate and up-to-date resources are used that are realistic, reflect pupils' lived experiences, and follow the latest pedagogical approaches, such as not employing scare tactics.
- All stakeholders are involved in the process, including pupils and parents.
- 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 does good practice look like:

- 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:

- Online safety is not clearly seen as a safeguarding subject.
- 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 use fear, shock or victim blaming approaches.
- The programme of study in place is not progressive or sustainable. For example, there is a substantial reliance on external providers/visitors to deliver online safety education and/or online safety education 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 is not aware of or cannot explain how the Department for Education's 'Teaching online safety in schools' guidance has been used 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 is 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 cannot explain how overlap is avoided between RSHE and Computing in order to avoid duplication or how the curriculum is flexibly adapted in line with the latest harms and incidents.
- 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'.

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
- London Grid for Learning (LGfL): https://onlinesafetyprinciples.lgfl.net
- NCA-CEOP Education - online safety education programme: 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

Part five: Whole school community engagement and education

Question to ask

- **How does the school/college engage and educate parents and the whole school/college community with online safety?**

Why ask 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."

KCSIE 2022 identifies that schools and colleges are likely to be in regular contact with parents and carers and communications should be used to reinforce the importance of children being safe online. For example, parents/carers are likely to find it helpful to understand what systems schools/colleges use to filter and monitor online use. Parents and carers should be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school/college (if anyone) their child is going to be interacting with online.

What evidence to look for:

- Engagement with parents/carers on relevant online safety content within the RSE and Health Education curriculum and consultation with them when policies are formed or updated.
- Regular communication, awareness-raising and engagement on online safety issues and reporting routes through using different communication channels such as social media, the school/college website and newsletters.
- Regular opportunities for engagement with parents on online safety issues, such as awareness workshops.

What does good practice look like:

- Parents/carers are proactively engaged in school/college activities that promote the agreed principles of online safety. For example, this may involve co-designing programmes to ensure parents' (and their children's) experience of emerging online issues are reflected.
- Interactive engagement with parents, with the aim of building skills, language and confidence to support their children in responding safely to online harms, as well as general awareness on online safety issues.

- Regular and appropriate online safety resources and sessions are offered to parents. Relevant resources will cover key online risks and behaviours displayed by pupils/students at different ages in the school/college.
- Evidence of pupils/students working with their parents to develop their understanding of online issues.
- Online safety information available in a variety of accessible 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 engagement or consultation with parents on online safety content as a part of RSE and Health Education curriculum
- No online safety engagement with parents.
- Out-of-date, inaccurate and/or purely reactive advice provided to parents.
- Recurrent concerning online behaviours amongst pupils/students (such as younger pupils playing games aimed towards older adolescents and adults).

Where to go for more support:

- CEOP Education: https://www.thinkuknow.co.uk/parents/
- NSPCC: https://nspcc.org.uk/keeping-children-safe/support-for-parents
- Parent Zone: http://parentzone.org.uk/
- UK Safer Internet Centre: https://saferinternet.org.uk/guide-and-resource/parents-and-carers
- DfE: 'Harmful online challenges and online hoaxes': https://www.gov.uk/government/publications/harmful-online-challenges-and-online-hoaxes

Annex A

Monitoring online safety: proforma

Policies and procedures
Does the school/college have up to date policies that address online safety, mobile and smart technology, social media and acceptable use of technology in place? **How does the school/college assess that policies are clear, understood and respected by all children and staff?**
Source(s) of evidence
Comments

Support and Reporting mechanisms
What mechanisms does the school/college have in place to support pupils/students, staff and parents facing online safety issues?
Source(s) of evidence
Comments

Staff training
How do you ensure that all staff receive appropriate, relevant and regularly updated online safety training?
Source(s) of evidence
Comments

Teaching and Learning

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 include 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.

Source(s) of evidence

Comments

Whole school community engagement
How does the school/college engage and educate parents and the whole school /college community with online safety?
Source(s) of evidence
Comments