UK Council for Internet Safety

Online Safety Audit for Trainee & Early Career Teachers

Before you start work at a new school, whether as a placement while you train, or as your first school as an Early Career Teacher, ensure you have the answers to these questions. You may wish to note the answers here for reference. Your school mentor and (if you are in training) your ITT provider have a responsibility to cover this vital and fast-moving area of safeguarding (online safety = safeguarding) but it is in your interest to show an active interest and ask lots of questions.

FIRST STEPS AND YOUR NEW SCHOOL

Have you read and understood the following?

- *Keeping Children Safe in Education* Part 1 and Annex C: Online Safety (Department for Education) ☐
- *Teaching online safety in school* (Department for Education) ☐
- Your new school's online safety policy ☐
  (NB this may be a standalone document or part of the overall safeguarding / child protection policy; equally it may be very different to other schools you have been placed in)
- School Behaviour Policy ☐
- Staff code of conduct and, if separate, acceptable use policy or AUP. ☐
  (NB These may all be part of a staff handbook; they govern how you use the school network and devices, how you behave online at school AND elsewhere, staff/pupil relationships and communications – including the use of social media)

To understand how online safety is covered in the curriculum, you may also find it useful to look at the online elements of the Relationships Education, Relationships and Sex Education (RSE) and Health Education curriculum, which includes many mentions of life online, as well as the relevant elements of Computing and the UKCIS framework Education for a Connected World.

Make a note here of the compulsory safeguarding sessions you attended at your ITT provider and your new school (this should be before you formally start work in the classroom), including date, trainer and which online safety elements were included.

_____
_____
_____
_____

Do you know how to identify a child who may be at risk of harm/or has been harmed, online or otherwise, as well as how to act upon concerns and disclosures, who to talk to and which policies/procedures to follow.

YES/NO

If you answered no or are in any doubt, please speak to your DSL immediately.

What questions do you have for your mentor and/or the designated safeguarding lead (DSL) or RSHE/PSHE lead about the documents you have read or the training you have attended? Don't just write them down - remember to ask them.

_____
_____
_____
_____
_____

Who are the DSLs at your new school, and any named online safety lead if different (remember overall responsibility for online safety remains with the DSL/s) and RSHE/PSHE lead who will be doing lots of curriculum preparation for online safety?

[insert name and role for each]

_____
_____
_____
_____
_____
_____
_____
_____

What is the process for reporting online-safety concerns in your school?

_____
_____
_____

WHAT IS ONLINE SAFETY?

What does online safety mean (don't Google it; write down your thoughts)? Is it different from digital resilience? And is there an online and an offline world?

_____
_____
_____
_____

What do young people today need to be equipped for in the online world that didn't exist a few years / a decade or two ago (and should be part of a balanced online-safety education)?

_____
_____
_____
_____

How might this be different for vulnerable pupils?

_____
_____
_____
_____

How can you stay up to date with the latest risks and opportunities in the digital world?

_____
_____

How is staying safe online at school different to staying safe online at home?

_____
_____
_____

How do you think online safety education might/should be different in a primary/secondary school (the opposite of the phase you teach in)?

_____
_____
_____
_____

A student in a focus group said, “I don’t go online; I just use YouTube and Snapchat”. What can we learn from this quote and how can we ensure that what pupils learn is relevant to their lives?

_____
_____
_____

Watch the video or read fof.lgfl.net, which shows ten statements that often crop up in online-safety lessons but which might be oversimplifications. Which do you agree with? Why/why not? Why does it matter what language we use in the classroom?

_____
_____
_____
_____

How can you balance planned curriculum online-safety education and making the most of opportunities to respond to pupils when they talk about digital aspects of their lives?

_____
_____
_____
_____

DAY TO DAY CURRICULUM

Do you have direct involvement in the delivery of the computing or RSHE/PSHE curriculum?
YES/NO

If YES above, where is your documentation about the approach, scheme of work / plans and your role in delivery (which will include much more detail than you can note here)?

_____
_____

If NO above, speak to the leads in these areas to ask them about the school’s approach to these subjects and what the pupils you teach are learning, how and when? Make notes here on what you found out / where information can be found:

_____
_____
_____
_____

For subject specialists (whether primary or secondary school), how does your subject contribute to whole-school teaching of online safety in the curriculum (this might be specific lessons or themes, or mentions whenever you do a certain activity or use devices, etc)? Where does it appear?

For form tutors (secondary), what opportunities are there to address online safety in an informal (when chatting with your tutees or overhearing a conversation) or structured way (assembly and form time even if you do not teach RSHE)?

For class teachers (primary), what opportunities are there to address online safety in an informal way (when chatting with your class or overhearing a conversation), and what are planned and ad-hoc elements of your termly plans that feature online safety?

For all the different roles mentioned above, have a conversation with an experienced colleague and make notes below about what you have learned from their experiences of both planned and ad-hoc online-safety learning opportunities. Feel free to include any ideas you have about generating more informal opportunities for discussion and learning.

How is online-safety learning assessed in your school (not only in RSHE/PSHE and Computing but in other subjects)?

How does your school identify and provide relevant online-safety learning to pupils with additional learning needs and vulnerabilities?

Parents often look to schools for support with online safety; it is an area that many feel ill equipped to handle. How does your school engage parents and what opportunities can you see to better involve and support ALL parents throughout the year (a 'drip-feed' rather than 'big-bang' approach is recommended).

_____
_____
_____
_____

What are the challenges of engaging and working with parents regarding online safety (e.g. age ratings for games / social media)?

_____
_____
_____
_____

YOUR ONLINE PRESENCE AND REPUTATION

It is important as a new teacher to consider your personal online reputation and whether your past, current or future digital presence could be deemed to 'bring the profession into disrepute', which could lead to disciplinary proceedings. Some things are not acceptable for teachers to share online; some are acceptable if private, but private images quickly become public online, so it is important to audit your online presence and privacy settings.

What do you think might cause problems for a teacher online? List a few different answers.

_____
_____
_____
_____
_____
_____

If you search for yourself online (using a search engine in a private browser tab which is not logged-in), what can anybody see? Are there any posts or images that could cause offence or embarrassment to you or your school? If so, what will you do about that?

_____
_____
_____

Have you changed your social media platform settings to private / friends only (where appropriate; some platforms are designed to be public)? ☐

For these platforms, remember that a parent or colleague from the school may become a friend of a friend and see a post that you think is private, or it may be shared without your consent, or the platform may change its settings.

If you use dating apps, be aware that this will be of great interest to your pupils and there have been instances of teachers being 'catfished'.

- Are you prepared for the risk a pupil trying to contact you using a fake profile? ☐
- It is perfectly acceptable for a teacher to engage in online dating, but would the images and language you use cause distress or disciplinary problems if they were circulated at your school? ☐

For public apps/platforms, are there any posts that a headteacher/governor or a parent of a child in your care might find inappropriate or offensive? It may be wise to ask an experienced/senior colleague or friends with children to check for you. ☐

Have you removed any posts / images / comments / likes that you think might be unwise? ☐

Do you need to ask for further advice or support? ☐

- From your school mentor ☐
- From your ITT mentor ☐
- From the online safety / safeguarding lead or other SLT at your school ☐
- From the Professionals' Online Safety Helpline (service from the UK Safer Internet Centre: 0344 381 4772 or helpline@saferinternet.org.uk ☐

Note here any questions you have or issues you plan to discuss:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

CASE STUDY

Read the following list - what do they have in common?

- ...told her he was 24 when he was 21
- ...exchanged one or more messages with Child A via text and/or Snapchat
- ...engaged in a phone call with Child A on one occasion or more
- ...sent Child A a photograph of himself on at least one occasion
- ...exchanged text messages, WhatsApp messages and Facebook messages with Student A on one or more occasions
- ...exchanged inappropriate messages with Student B about Student A
- ...sent his personal contact details
- ...sent inappropriate messages
- ...disclosed personal information
- ...accessed her school email account in order to send her messages
- ...deleted emails he had exchanged with Pupil A
- ...instigated a discussion with him via Instagram
- ...used his personal mobile phone to take and store images relating to school activities
- ...used his personal laptop to search for websites and/or material involving sexual activity with children
- ...took inappropriate photos of one or more pupils without their knowledge
- ...stored photos of pupils from the School on one or more personal devices
- ...viewed and/or obtained inappropriate and/or sexual material through the college's technology
- ...made comments of a sexual nature to Pupil A
- ...gave Pupil A his personal number
- ...shared details of his personal life with Pupil A
- ...sent her one or more nude image of yourself
- ...failed to follow advice and/or warnings […]in relation to not contacting pupils using personal mobile phones

These were all evidence used in career-ending prohibition cases where teachers were banned from the teaching profession as a result of unprofessional behaviour. Whilst some are obviously wrong in any circumstance and enough to prompt an investigation or even arrest, some might be permissible in one school in certain contexts and/or with permission...but lead to disciplinary proceedings in others.

The serious consequences of inappropriate behaviour on social media are underlined by the fact that there have been **200 Prohibition Orders** issued to teachers over the past four years related to the misuse of technology/social media.

Are any of the points above unclear to you? Highlight or underline any you don't understand so you can discuss with your mentor.

Are you unsure about any of the points above at your new school (e.g. personal device / account use in school)? Take a note here and find out the answer from your mentor:

_____
_____
_____
_____

Remember that you should not be friends with pupils on social media or follow their accounts unless this is clearly part of your school policy (this is rare and will have strict parameters to protect you by ensuring other staff can see your communications for your protection). If pupils follow you on a certain platform and this is not avoidable, you should declare this to your school. Equally if you have any existing relationships which would otherwise be inappropriate (e.g. Facebook friends with a pupil as they are a family friend or relative). Is there anything you need to declare to your school in this respect?

_____
_____
_____

REFLECTIVE QUESTIONS

The following questions are written to help you identify any areas that you need to adapt your practice, find out more or otherwise reflect upon to keep yourself and the children and young people in your care safe.

When are you allowed to use or carry on your person or personal mobile device at school? What are the restrictions for general private use on school site?

_____
_____

What about wearable tech (including but not limited to smart watches, whether they can only be used to view messages or can capture audio, photo and video material)?

_____
_____

Are you allowed to use your personal device (mobile phone, laptop, etc) to access school emails / data? What are the restrictions / what is allowed?

_____
_____

When / are you allowed to take photos or videos of pupils or their work, whether for documenting progress, class displays or school marketing, etc.? What are the restrictions? Where do you find names and levels of pupil photo permissions?

_____
_____

Why might a child be at risk of serious harm if an image is shared without parental/carer consent?

_____
_____

Can you ever use your personal device to take photos at school or of pupils, events or trips? What are the restrictions (you might be allowed to take photos of homework, but not of pupils, for example)?

_____
_____

Be aware that if you use a personal device to take photos in school you may be required to surrender it for inspection.

How do you maintain a work-life balance, including when do you turn off work emails and what is your school policy on this (the Department for Education has a template email policy in its workload toolkit - if your school doesn't, you could show this to your mentor)?

_____
_____

NEXT STEPS

What 5 things are you now going to do (or do differently) as a result of this audit?

_____
_____
_____
_____
_____

What 5 areas/themes things do you need to find out more about?

_____
_____
_____
_____
_____

Are there areas in which your school could improve its online safety education or support for pupils and parents (for example, is there a discrepancy between policy and practice or between safeguarding and curriculum messages)?

_____
_____
_____
_____

FURTHER RESOURCES

The following organisations provide support, guidance and training (including template policies, online reputation guidance and parental support portals) to teaching professionals that will help you develop your understanding of online safety issues:

NCA CEOP
Childnet
UK Safer Internet Centre
LGfL
Parent Zone
NSPCC
The Education People **(formerly Kent CC)**

This document has been developed by the UKCIS Education Working Group, which is made up of the following organisations: