Online Safety Guidance for the Full Opening of Schools

It is planned that all pupils, in all year groups, will return to school full-time from the beginning of the autumn term 2020. This guidance is intended to support schools to consider and prepare for potential online safety action required.

Filtering and monitoring systems

Whilst unlikely, it is possible that changes to filtering and monitoring system may have taken place since schools were last fully open. It's advised that schools check systems and approaches before all children return to ensure they still comply with pre Covid-19 approaches and that appropriate filtering and monitoring policies and systems are operational in line with 'Keeping Children Safe in Education' (KCSIE) 2020 requirements.

Where technical checks are required, it's likely that technical staff will require time and space; this should be carried out in line with any social distancing requirements at the time and remote updates should be carried out where possible.

- SWGfL provide a tool for schools to use to check if their filtering is compliant.
- UK Safer Internet Centre provide guidance on 'Appropriate Filtering and Monitoring

User issues

It's possible that some staff and learners will need technical support when returning to site e.g. passwords for systems may have expired or been forgotten. Activities are likely to be required to be undertaken by technical staff; this should be carried out in line with any social distancing requirements at the time. IT staff may require additional time and space to carry out these tasks and this should be timetabled in where possible.

Schools may need to revisit their existing security requirements with staff and learners e.g. not sharing passwords, locking screens, reporting scam emails, not installing applications without permission.

Online safeguarding policies and procedures

Staff

Staff should be reminded of existing procedures and expectations, as this may have been different during remote learning situations or may have been revised by the school. This should include:

- Acceptable Use of Technology Policy (AUP) as part of the school's behaviour policy/code of conduct
- Use of social media
- Image use
- Anti-bullying policy
- Mobile technology policy e.g. if personal devices are or are not permitted, and what behaviour expectations are in place
- Internal and external online safety reporting mechanisms e.g. reporting to the DSL etc.

Staff should also be reminded of:

- the school's IT classroom management expectations e.g. age/ability appropriate supervision, pre-checking search terms, using age/ability appropriate tools.
- the procedures to follow when responding to peer on peer abuse concerns.

Children

At a level appropriate to their age and ability, learners should be reminded of existing procedures and expectations, as this may have been different during remote learning situations or may have been revised by the school. This should include:

- Acceptable Use of Technology Policy (AUP) as part of the school's behaviour policy/code of conduct
- Anti-bullying policy
- Mobile technology policy e.g. if personal devices are or are not permitted, and what behaviour expectations are in place
- Internal and external online safety reporting mechanisms e.g. speaking to a member of staff, who the DSL is etc.

Acceptable Use of Technology Policy (AUP) and Mobile Technology and Social Media policy templates can be found on Kelsi. Further advice can be sought from the Education Safeguarding Service.

Social media considerations

During Covid-19 restrictions, many schools will have increased their use of social media as a communication tool. Schools should ensure decisions and behaviour expectations regarding use of social media are clearly documented.

Schools are required to address communication and use of social media in their policies e.g. the staff code of conduct. Schools should review their policies and ensure official and personal use of social media is addressed; for example, staff should not use personal social media accounts to communicate with learners and/or parents.

- Further advice can be sought from The Education Safeguarding Service.
- A template social media policy and AUPs is available for schools to adapt on Kelsi.

Content shared on social media requires planning as it can lead to several safeguarding risks, such as blurring of professional boundaries and risk of vulnerable children/parent being identified. Schools should undertake a risk assessment approach when implementing official use of social media to ensure all reasonable safeguarding precautions are taken.

- Advice regarding official social media use can be sought from the Education Safeguarding Service.

Increase/decrease in online safety concerns being reported

Some learners may have encountered online risks whilst off site but felt unable to or were unaware of how to report concerns; this could mean an increase in reports as children return to school. Additionally, it is possible children will not be taught by staff they have relationships with, so feel less able to report concerns.

- Review existing age/ability appropriate internal reporting mechanisms for learners and consider if they can be implemented safely e.g. talking to a member of staff, reporting to DSL, use of a dedicated reporting email, 'worry boxes', peer support.
- Remind children online site of age/ability appropriate external online safety reporting mechanisms e.g. Childline, CEOP, IWF, Report Harmful Content etc.
- Share online safety advice and reminders of reporting mechanisms with children and parents/carers.

Safeguarding consultations for Kent Schools can be sought from the Education Safeguarding Service and additional resources can be found via the TEP blog: Online Safety links and resources to share with staff and parents/carers.

Safer remote learning

Where children are being asked to learn online at home, such as a need to self-isolate, a local lockdown, or when complying with clinical and/or public health advice, schools need to ensure they can access remote learning safely. Schools will need to consider how best to manage remote learning and should implement the approaches which best suit the needs of their children and staff. This should include the age and ability of learners and IT provision and access.

The following safeguarding advice will help school manage safeguarding risks when providing remote learning, including when sharing live video/audio or pre-recorded content.

General recommendations for safer remote learning

- Any platforms or systems used should be approved by SLT prior to any use with children.
    - It is recommended schools use existing video conferencing tools/platforms where possible, as they should have already been evaluated and have any necessary parental consents.
    - New platforms or systems should be risk assessed and approved by SLT prior to any use.
        - Education specific or commercial products which offer more control should be used rather than free or home use versions.
        - Risk assessments should take place from a technical, curriculum, data protection and safeguarding point of view.
- Platforms should be set up securely by the school to prevent unauthorised access.
- Resources used should be used in line with existing teaching and learning policies, taking licensing and copyright into account.
- Any personal data used by staff or captured or used when delivering remote learning must be processed and stored with appropriate consent and in accordance with data protection requirements e.g. GDPR and school policy.
- Staff, parents and children should be made aware they need to follow school policies and procedures e.g. child protection, acceptable use of technology (AUP) and behaviour.
    - Policies and procedures may need to be updated to reflect new technology use and behaviour expectations.
    - Deliberate misuse should be responded to in line with existing school policies.
    - Welfare concerns about any children should be brought to the attention of the Designated Safeguarding Lead (DSL) without delay.
    - Any concerns about members of staff should be reported to the headteacher.
- Staff should:
    - use school provided devices e.g. laptops, tablets and phones where possible.
        - If this is not possible, SLT should ensure clear expectations are in place, for example restricting access, locking devices, blocking/withholding personal phone numbers, logging times/dates of contact and not taking or recording images for their own personal use.
    - use school approved communication channels or platforms only.
        - Staff should not use personal accounts or social media channels to provide remote learning or support.

    - receive training prior to using platforms/systems which explores how to use key functions as well as behaviour expectations.
- Children should:
    - use official school managed accounts to access remote learning.
    - be reminded of remote learning behaviour expectations.
- Parents/carers should be:
    - made aware of what their children are being asked to do online, including the sites they will be asked to access.
    - aware of who (if anyone) from the school, their children are going to be interacting with online.
    - encouraged to ensure children are appropriately supervised online and that appropriate parent controls are implemented.

General recommendations for live streamed sessions

- Platforms should be set up securely to prevent unauthorised access e.g. password protect live streams and use 'waiting rooms' or 'lobbies' to restrict access.
- Live sessions should be planned and scheduled during school hours.
- Staff should record the length, time, date and attendance of any live sessions held.
- A member of SLT, the Designated Safeguarding Lead or another senior member of staff should have the ability to 'drop into' live lessons where possible.
- Parents should be aware that live sessions are taking place and ensure that their child is appropriately supervised.
- If schools opt to 'record' live streamed sessions, all participants should be made aware that the session is being formally recorded. Schools should ensure recording and keep, stored and accessed in line with existing data protection requirements.
- Schools should be aware that other household members may be present during live sessions, for example staff's family members or children's sibling/parents.
    - Clear expectations should be shared with the whole community to ensure anyone who can be seen and/or heard during live sessions is suitably clothed, uses appropriate language and does not share sensitive/personal information.
- School should assess if it necessary for children to use live video, microphones or text-based chat when remote learning.
    - These functions may need to be disabled according to school decision and context e.g. age/ability of children. If they are enabled, school should evidence any action taken to minimise or remove risks.

Note: DfE Coronavirus (COVID-19): safeguarding in schools, colleges and other providers May 2020 states that there is no expectation that teachers should live stream or provide pre-recorded videos.

Recommendations for one-way communication e.g. only teacher live streams video and/or shares screen with audio

- Where possible two members of staff should be present in live streamed sessions.

    - One member of staff should be responsible for delivering content and the other provide support and safeguarding assistance if required, for example monitoring children's interaction.
    - If this is not possible, schools should evidence the decision making and outline action taken to reduce risks.
- Clear boundaries as part of an updated or specific AUP should be in place:
    - Staff behaviour and language use during live sessions should be in line with the staff behaviour policy/code of conduct.
    - Staff should dress professionally and use a neutral background for their video stream. If possible, enable background blur tools when live videos are being shared.
- Consider reducing live camera time e.g. staff talking over PowerPoint slides or sharing work demonstrations rather than video streaming.
- Disable children's video/audio if possible, or ensure staff have control over cameras/microphones functionality.
- Children should be encouraged to access the live stream from a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.

Recommendations for two-way communication e.g. teacher can see/hear children and children can see/hear each other

- Two members of staff should be present in sessions.
    - One member of staff can deliver curriculum content whilst the other provides behaviour/technical support and safeguarding assistance if required e.g. monitoring children's videos and any chat if not disabled.
- Children should be provided with clear boundaries and expectations. They should:
    - dress appropriately e.g. clothes they might wear for a non-uniform day, not pyjamas.
    - behave as they would in the classroom.
    - live stream from a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.
    - ensure there is a neutral background to their videos or use background blur options.
        - Note: If schools allow children to upload their own background rather than use default images, clear expectations about what is appropriate should be in place.
    - Schools should control children's video/audio features.
        - Schools should prevent children from turning their camera/microphone on themselves where possible, depending on their age and needs.
        - Where possible, schools should restrict children's access to chat and/or video functions after a live session has ended.

Recommendations for 1:1 sessions between member of staff and child

Schools should avoid 1:1 sessions between children and staff where possible, however, Safeguarding and remote education during coronavirus (COVID-19) states '*Schools might want to consider whether one-to-one sessions could be appropriate in some circumstances. For example, to provide pastoral care or provide support for pupils with special educational needs and disabilities*.'

If a school decide it is appropriate and necessary to facilitate 1:1 sessions, to reduce risks:

- If a session does not require confidentiality e.g. for tuition, two adults should be present if possible.
    - For example, a member of staff could be on site with another member of staff present in the room. The 2nd member of staff does not have to be involved in the session, but children should be made aware they are present. Alternatively, a parent/carer could remain in the room with the child whilst the session takes place.
- This will not be possible in all circumstances, or if particularly sensitive conversations (for example to provide pastoral care, counselling etc.) are taking place. If this is the case, the session should:
    - be risk assessed and approved by SLT.
    - be auditable e.g. the member of staff logs time, date and attendance.
    - Only take place using school provided equipment, platforms and accounts.

Recommendations for using pre-recorded content created and shared by the school

In addition to the general recommendation, risks can be reduced if schools:

- require staff to plan, rehearse and review videos to ensure content in line with school expectations
- consider auditing pre-recorded content before it is shared with children.
    - Schools may opt to check all pre-recorded content or audit a selection of material.
    - Content could be reviewed by SLT or another appropriate member of staff e.g. subject lead.

Note: DfE Coronavirus (COVID-19): safeguarding in schools, colleges and other providers May 2020 states that there is no expectation that teachers should live stream or provide pre-recorded videos.

Recommendations if using live streamed or pre-recorded content from other providers

Where schools are directing children to content from another provider, they need to ensure it is suitable and appropriate. Risks can be reduced if schools:

- only use content from providers who have a specific and up-to-date child protection policy in line with DfE guidance.
    - The DSL should be satisfied that the providers child protection policy and procedures are in line with the current 'Keeping Children Safe in Education' guidance.
- have a member of staff join any 'live' sessions so they can monitor the content and the interactions/behaviour of the children as they would within a school environment.
- ensure the platform being used is safe and appropriate e.g. live chat is managed and/or moderated.
- make appropriate checks to ensure any staff delivering the content are suitable (e.g. DBS checked)
- monitor a selection of sessions and/or content to check they are being conducted appropriately.

Additional Advice

Kent schools and settings can seek advice through the Education Safeguarding Service.

Guidance and resources to support schools can be found at:

- Remote Learning Guidance
- AUP for remote learning and communication
- Online Safety links and resources to share with staff and parents/carers

National guidance

- DfE: ‘Safeguarding and remote education during coronavirus’ (COVID-19)
- NSPCC: Undertaking Remote Teaching Safely
- National Cyber Security Centre: Video Conferencing Services
- SWGfL: Safe Remote Learning
- LGfL: Safeguarding during Covid-19