All Saints Schools Trust

Online Meeting Software Policy
2023-2027

Scope of the Policy

This policy applies to all All Saints Schools Trust staff including the Trustees, Members, Governing Bodies, all teaching and other staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

Background

As a result of the Covid-19 lockdown during 2020, schools across the Trust have been innovative with their practice in providing home learning for pupils. This has included the use of a variety of technologies that link home and school. A list of these, with increasing levels of risk, is shown below:

i) Links to resources through school website, messenger service and learning platform e.g. Purple Mash.
ii) Asynchronous approaches such as publishing videos of lesson introductions on YouTube.
iii) Live teaching sessions that take place in real time using software such as Zoom, Microsoft Teams, Skype and Google Hangouts.

The first two approaches have been used by schools for some time and this is reflected in current documentation. However, since 'live teaching' is a relatively new phenomenon, this guidance has been produced specifically to be used as a supplement to current school policies such as 'Online Safety' and 'Acceptable use of Technology'.

Risks

Whilst there are many benefits for using technology to enhance home learning, there is no doubt that live teaching presents risks of both a safeguarding and professional nature. These include the following:

- Any user could share inappropriate content that would be viewed by the whole group.
- Access could be granted to someone outside the group if the meeting is insecure or codes are leaked (known as zoom bombing).
- Background images may reveal personal information about teachers or pupils.
- All users have the capacity to screenshot/record the meeting showing the names and faces of pupils, some of which may be vulnerable. This raises data protection issues.
- Parents could challenge the presenter on their teaching during a lesson.
- Some online meeting apps use invasive tracking software.
- Apps such as Zoom, Teams and Skype are considered as "medium risk" across the board: for exposure to sexual content; violence and hatred; bullying suicide and self-harm; and drink, drugs and crime.

Baring the above in mind, the Trust advises the following precautions as a minimum:

1. Schools must have parent permission and ideally the meeting is mediated through them (particularly with very young pupils). Parents need to accept the risks involved in this medium.
2. No 1:1 lessons should take place, groups only. If catch-up teaching is recommended in the future, then the staff member should be accompanied by another member of the school team.
3. Staff and children must wear suitable clothing, as should anyone else in the household.
4. Any computers used should be in suitable areas without anything inappropriate in the field of view. Staff should consider using the features that blur or replace the background.
5. Language must be professional and appropriate, including any family members in the background who could be overheard.
6. Videos might need be muted for both pupils and staff if other children in the household become unsettled or cause a disruption.
7. To ensure all the of the above are possible, <u>it is essential</u> that staff spend the necessary time familiarising themselves with all the features e.g. testing the software with other teachers before using with pupils.

The following section contains advice from the NSPCC that Trust expects all schools to follow. The guidance is based on Zoom but should be applied to any equivalent app.

Keeping pupils safe in online lessons

Advice from NSPCC

Where possible, teachers should remain on the line with students throughout the call, and ensure all necessary safety features are in place to prevent unwanted intrusions. This could include turning off the screen-sharing feature and admitting students into the call one at a time.

i) **Secure your room**
If your class has started and all your pupils have arrived, you can lock your virtual classroom, so that no one else can join. Allow only recognised users to join. When using Zoom, generate a random meeting ID when scheduling your event and require a password to join.

ii) **Never publicise your meeting's link online**

iii) **Use virtual waiting rooms**
Use this feature to hold potential participants in a separate "waiting room", so you can check who they are before allowing them entry.

iv) **Limit screen sharing**
Make sure your pupils don't take control of the screen and prevent them from sharing random content by limiting screen sharing, so only you as the teacher (host) can present to the class until safe routines are established. Hosts can block unwanted, distracting or inappropriate noise/gestures from other participants by muting them or switching video off. Some apps allow you to have these off on default as people join.

v) **Remind pupils not to share personal information during meetings**

vi) **Disable private messaging**
Prevent distractions among your students by stopping private messaging between pupils, so they can't talk to one another without your knowledge.

vii) **Remove participants**
If inappropriate conduct occurs the participant should be removed from the meeting and the incident should be logged using the school's 'online safety' or safeguarding procedures as necessary. The teacher may feel that is necessary to end the session at this point.