Risk Assessment for Livestreaming school content

Risk	Mitigation
Inappropriate behaviour or conduct from adults, whilst using Teams	All sessions on Teams recorded and automatically uploaded to OneDrive. They can be deleted from a Team but are still accessible, if necessary, through ICT support. Staff instructed on the importance of recording.
Inappropriate behaviour or conduct from students	Cameras turned off and all mics muted at start of lesson as a default (can unmute if invited). KS3 do not have camera access. Some KS4 and KS5 students have asked for cameras to be enabled (e.g. Drama students). This has been allowed but has been discussed with families beforehand. Staff have the ability to turn off microphones or cameras to any student or group behaving inappropriately. In extreme circumstances, staff can remove a student from a lesson or remove their chat function. Parents or carers would be informed via Go4Schools. School has adapted a remote learning behaviour policy.
Unauthorised sharing of recording by pupils, parents, or staff	Clear guidelines (Code of Conduct) for all families and staff in our bulletins. Instances of misconduct reported on Go4Schools and followed up by pastoral teams as appropriate. Be aware of who has been assigned the current 'Presenter'. Be aware of what is safe to share within the specified Team.
Inappropriate contact with pupils outside lesson time	Clear guidelines on internet safety and security shared with staff, students and families; this is reiterated regularly through staff and family bulletins and the safeguarding policy. Monday morning briefings for staff used for reminders of this nature. Reporting and follow up of misconduct by staff to Safeguarding Lead / Deputy Safeguarding Lead. Reporting and follow up of misconduct by students to HOY.
Inappropriate contact with pupils in a different account or a different platform	Clear guidelines on internet safety and security shared with staff, students and families. This is reiterated regularly through staff and family bulletins. No student or employee to use personal email or personal social media accounts for contact.

	The 'lobby' settings, which potentially enable external visitors to access lessons, has default settings which mean that nobody without a Wales High School account can access lessons. Staff have been instructed to not alter these settings.
Inappropriate language in chat function	Extensive guidance (Code of Conduct) shared with families in bulletins, assemblies and active tutorial about appropriate use of the chat bar. Instances of misconduct recorded on Go4Schools and followed up by pastoral or departmental teams, as per the remote learning behaviour policy. If persistently abused, the chat function can be removed for individuals or groups.
Inappropriate dress, conduct, or location	All student cameras turned off by default. Some KS4 and KS5 students have asked for cameras to be enabled (e.g. Drama students). This has been allowed but has been discussed with families beforehand. Cameras are optional for staff and all have been briefed on the need for professional dress and background settings as part of their Teams training.
Unauthorised people invited into the video call (Teams)	GDPR Policy in place to prevent sharing of sensitive data outside of the organisation. External visitors are sometimes used in a lesson (e.g. Super Learning Days) but these are monitored by a host teacher at all times. Attendance is tracked and monitored at each remote lesson.
Unauthorised people crashing into video call (Teams)	The 'lobby' settings, which potentially enable external visitors to access lessons, has default settings which mean that nobody without a Wales High School account can access lessons. When a link to Teams meeting is shared by someone outside the organisation, it will not enable them to enter a session without bypassing the lobby. Permission is needed from the presenter in this instance. This means no unauthorised access to lessons, even with a link. School has tightened up protocol for students who are no longer on roll (e.g. email accounts disabled immediately so they can no longer access Teams). Invites to internal Teams can only be sent out via Team owner. Invite links can still be forwarded to unauthorised users – owners can remove user from Team.
Unauthorised streaming to another platform	Invites to internal Teams can only be sent out via Team owner. Invite links can still be forwarded to unauthorised users – owners can remove user from Team.
Unauthorised streaming to the wider public	Be aware of who you have invited to the Team, remove any unauthorised guest access.

Data breach. For example, showing pupils on camera without permission, sharing personal data	GDPR policy in place and staff are trained annually. The school has a 'no photos list,' which all staff must refer to if considering sharing images of students. All staff are provided with encrypted memory sticks and sensitive data to be saved on school systems (or OneDrive) and password-protected. Only certain pupils have been assigned the policy to use the camera, these have had permission from parents.
Data breach showing confidential information whilst online (e.g. email, social media etc.)	GDPR policy in place and staff are trained annually.
Unauthorised sharing of inappropriate content via share screen (e.g. as part of a live lesson)	Staff training on Teams has been provided for all staff. Extensive Teams guides, accessible for all staff, are provided regularly and weekly bulletins also reference this. Make sure presenters are aware of how to share content, windows and screen properly.
Accidentally being online early or afterwards without being aware	Code of conduct has been shared. Students and families told not to do this. Remote learning behaviour policy to deal with this.
Unauthorised chats or video whilst monitoring adult is offline	Code of conduct has been shared. Students and families told not to do this. Remote learning behaviour policy to deal with this. Permissions in place to revoke one-to-one chat and video whilst not within the Team meeting.
What action is to be taken if a disclosure or concern is raised by pupil whilst online?	Follow safeguarding policy.
How will concerns be raised about any livestream issues by pupils, parents or staff?	Safeguarding and pastoral policies / e-safety policy published on website and reviewed for remote learning – shared weekly with staff and families.
Errors, mistakes, or concerns should be self-reported. How should this be done?	Weekly SLT link meetings (with a subject or pastoral leader and their line manager) is a forum for such discussions. Issues regarding online errors can also be dealt with by contacting ICTsupport@waleshigh.com. Safeguarding issues through safeguarding team.