Muswell Hill Primary School

Remote Teaching and Online safety in schools – Safeguarding Online Child Protection Policy Addendum updated January 21

Please read in conjunction with the following: Safeguarding & Child Protection Policy, Blended Learning Policy & Practice, Remote Learning Policy, Behaviour Policy Addendum, Anti-bullying Policy

Remote Learning

We will continue to provide a safe environment for our pupils, including online. Where pupils are using computers in school, appropriate supervision will be in place.

Children and online safety away from school

It is important that all staff members who interact with children, including online, continue to look out for signs that a child may be at risk. Any such concerns should be dealt with according to the school's Safeguarding Policy and where appropriate referrals should still be made to Haringey MASH (or its equivalent in another LA if the child resides in a different LA) and/or the police immediately.

Online teaching follows the same principles as set out in the Staff Code of Conduct. We will ensure any use of online learning tools and systems is in line with privacy and data protection law requirements.

Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- No one-to-one sessions, teach in groups only. *(exemptions relating to supporting vulnerable children not in school, on a one-to -one basis, should only take place if previously agreed with parents and SLT).* NB. All considerations below still apply.
- Teachers should be in a neutral area where nothing personal or inappropriate can be seen or heard in the background.
- Staff and children must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, for example, not in bedrooms; and where possible be against a neutral background. When using Zoom Education, adults turn on blurred background and request this for all children also.
- The live class should be recorded and backed up elsewhere, so that if any issues were to arise, the video can be reviewed.
- Live or recorded classes should be kept to a reasonable length of time, or the streaming may prevent the family ‘getting on’ with their day.
- Language must be professional and appropriate, including any family members in the background.
- Schools should risk assess the use of live learning using webcams.
- Schools must reassure themselves that any teaching/learning software and/or platforms are suitable for the age groups and raise no privacy issues; or use cases against the provider’s terms and conditions (for example, no business use of consumer products).

Remote learning rules

Expectations for pupils at home - if pupils are not in school, we expect them to follow all of the rules set out below.

Parents should also read the rules and ensure their children follow them. Parents should contact one of the Senior Leadership Team, if they think their child might not be able to comply with some or all of the rules, so we can consider alternative arrangements with them.

Children should:

- Be contactable during required times – although take into account that pupils may not always be in front of a device the entire time.
- Complete work to the deadline set by teachers.
- Seek help if they need it, from teachers or teaching assistants.
- Alert teachers if they're not able to complete work.
- Use proper online conduct, such as using appropriate language in messages.
- Avoid being in bedrooms when completing sessions and should always be supervised by an adult to avoid 'wandering' with devices during live sessions.
- Parent/carer or supervising adult MUST be present and in the same room when their child is having contact with their teachers and their peers.

Digital Online Etiquette:

- ALL sessions will be recorded.
- Children mute themselves when they are not speaking.
- Children will be on time.
- Grown-ups check the technology is working before the sessions.
- All children, staff and adults in the household wear suitable clothing.
- To speak, children raise their hand or type S in their chat button.
- Children should look into the camera.
- Children should be supported to stay focused and show good speaking and listening.
- Teachers will go through the Classroom Zoom Rules before each session.
- Parents must sign an agreement to confirm they will supervise and reinforce MHPS online etiquette.

Remote Learning Behaviour Expectations: (Please refer to Behaviour Policy Covid 2021 Addendum)

The following guidelines for pupil conduct when remote learning (at home or at school) should be followed.

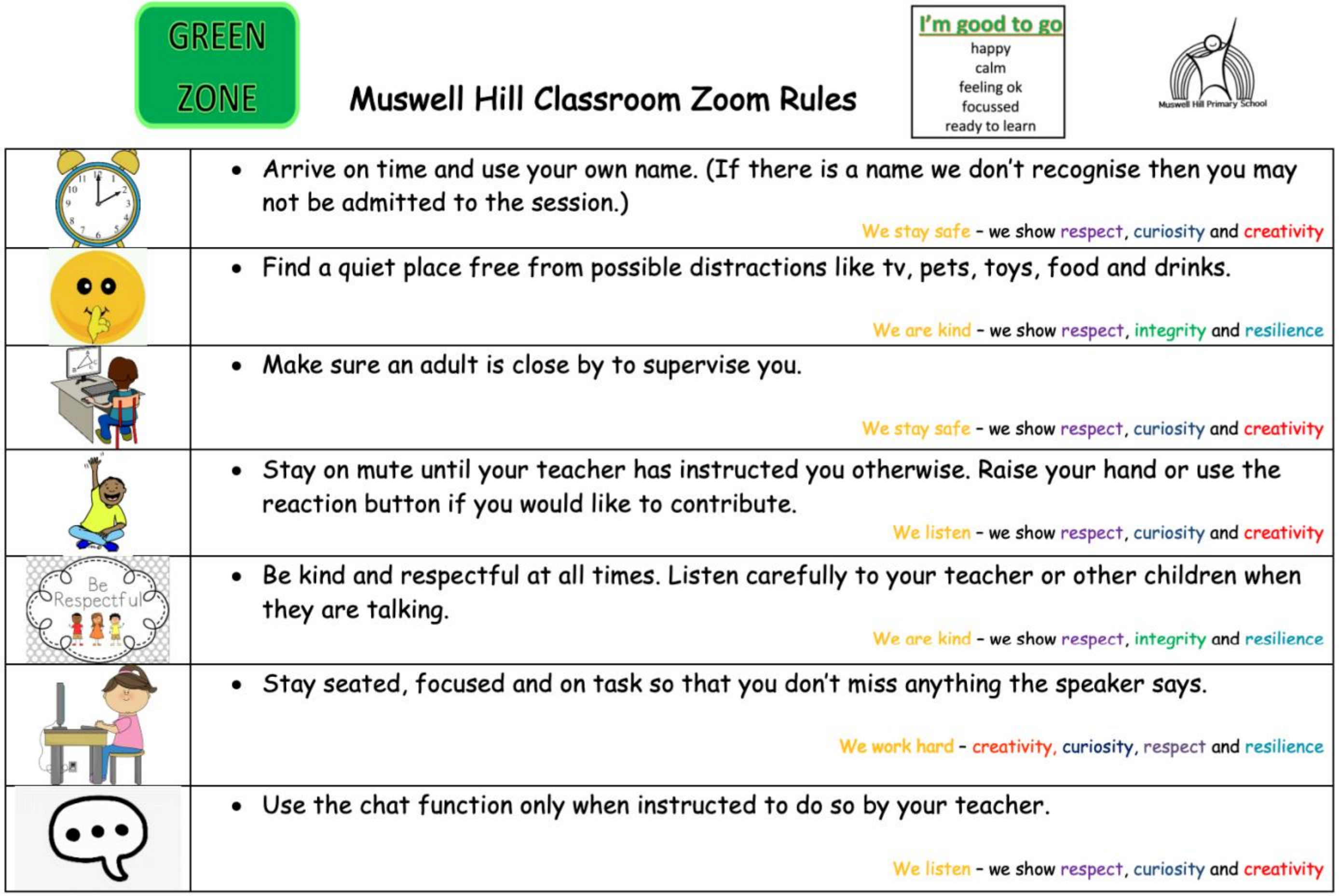
Pupils should

- treat remote learning in the same way as normal classroom learning where they can.
- if interacting with other pupils or staff online, students should always be kind and respectful to each other and be respectful and obedient to staff, remembering always that that staff are not 'friends' with, or peers to, pupils.
- pupils should never attempt to contact staff via social media or make comments about staff on social media platforms.
- any inappropriate comments to staff online, via Seesaw, or any other platform will be taken very seriously, and sanctions applied.
- any online bullying towards other pupils or peer-on-peer abuse that is disclosed to the school during this time will be taken very seriously and sanctions applied.
- use appropriate classroom language.
- take regular screen breaks.
- only communicate through approved school portals and platforms (seesaw, school email and zoom).
- do not use school platforms to discuss personal matters or make private comments in the chatroom.
- follow the teachers' guidance on audio and video use when on zoom sessions. If rules are not followed it may result in you having to leave the session
- be made aware that the lesson is being recorded.
- report any inappropriate use to their teacher or a trusted adult.
- do not share passwords or other sensitive information online.
- look after their mental health and wellbeing and ask for help from their teacher or other trusted adult if they need it.
- Additionally, normal school policies and expectations apply.

The School expects all staff and pupils to show kindness, and respect to other members of the community always.

Please see below for MHPS rules for the **Zoom Classroom Environment.**

This, and a version for parents and carers, are available on the school website or from the school office.



GREEN ZONE

Muswell Hill Classroom Zoom Rules

I'm good to go
happy
calm
feeling ok
focussed
ready to learn

Muswell Hill Primary School

	• Arrive on time and use your own name. (If there is a name we don't recognise then you may not be admitted to the session.) We stay safe - we show respect, curiosity and creativity
	• Find a quiet place free from possible distractions like tv, pets, toys, food and drinks. We are kind - we show respect, integrity and resilience
	• Make sure an adult is close by to supervise you. We stay safe - we show respect, curiosity and creativity
	• Stay on mute until your teacher has instructed you otherwise. Raise your hand or use the reaction button if you would like to contribute. We listen - we show respect, curiosity and creativity
Be Respectful	• Be kind and respectful at all times. Listen carefully to your teacher or other children when they are talking. We are kind - we show respect, integrity and resilience
	• Stay seated, focused and on task so that you don't miss anything the speaker says. We work hard - creativity, curiosity, respect and resilience
	• Use the chat function only when instructed to do so by your teacher. We listen - we show respect, curiosity and creativity

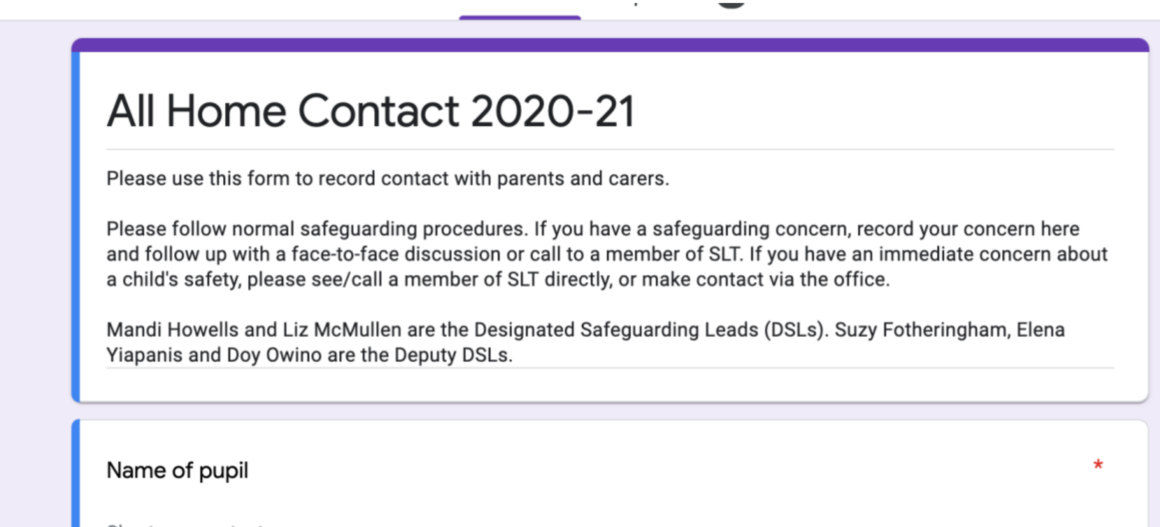
Supporting children not in school

Muswell Hill Primary School is committed to ensuring the safety and wellbeing of all its pupils. Where the DSL or Head of School has identified a child to be on the edge of social care support, or who would normally receive enhanced pastoral or educational support in school, we will ensure that robust communication is in place for that child or young person. Details of any communication, will be recorded on Google Docs and will be reviewed regularly. Any concerns arising during remote learning support, including 1:1 or group tutoring, will be reported to the DSL(s) as per normal safeguarding practices.

The school will share safeguarding messages through the leadership team messages to pupils and parents and through newsletters, letters and SeeSaw communication.

We recognise that school is a protective factor for children and young people and the current circumstances can affect the mental health of pupils and their parents/carers. Teachers and staff ~~at the school~~ need to be aware of this in setting expectations of pupils' work where they are at home.

As agreed with members of SLT, where 1:1 check-ins or lessons are being provided for vulnerable pupils, staff will record their contact with children via Google Forms:



All Home Contact 2020-21

Please use this form to record contact with parents and carers.

Please follow normal safeguarding procedures. If you have a safeguarding concern, record your concern here and follow up with a face-to-face discussion or call to a member of SLT. If you have an immediate concern about a child's safety, please see/call a member of SLT directly, or make contact via the office.

Mandi Howells and Liz McMullen are the Designated Safeguarding Leads (DSLs). Suzy Fotheringham, Elena Yiapanis and Doy Owino are the Deputy DSLs.

Name of pupil *

Supporting children in school

Muswell Hill is committed to ensuring the safety and wellbeing of all its pupils. We will continue to be a safe space for our pupils to attend and flourish. The safeguarding team will ensure that appropriate staff are on site and staff to pupil ratio numbers are appropriate, to maximise safety. We will refer to the Government guidance for education and childcare settings on how to implement social distancing and continue to follow the advice from Public Health England on handwashing and other measures to limit the risk of spread of COVID19. We will ensure that, where we care for children of key workers and vulnerable children on site, the appropriate support is in place for them. This will be bespoke to each pupil and recorded appropriately.

Zoom Education Usage – Advice for Staff

Protecting your Meeting

The following in-meeting security capabilities are available to the meeting host:

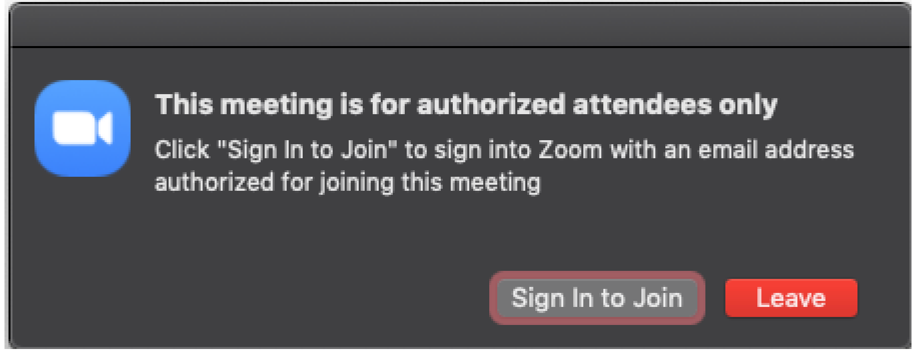
- Secure a meeting with encryption
- Create Waiting Rooms for attendees
- Require host to be present before meeting starts
- Expel a participant or all participants
- Lock a meeting
- Screen share watermarks
- Audio signatures
- Enable/disable a participant or all participants to record
- Temporary pause screen-sharing when a new window is opened
- Password protect a meeting
- Only allow individuals with a given e-mail domain to join

https://zoom.us/docs/image/new/security/img-protectingmtg.png

Manage your participants

Some of the other great features to help secure your Zoom event and host with confidence:

- Allow only signed-in users to join: If someone tries to join your event and isn't logged into Zoom with the email they were invited through, they will receive this message:



This meeting is for authorized attendees only

Click "Sign In to Join" to sign into Zoom with an email address authorized for joining this meeting

This is useful if you want to control your guest list and invite only those you want at your event — other students at your school or colleagues, for example.

- Lock the meeting: It's always smart to lock your front door, even when you're inside the house. When you lock a Zoom Meeting that's already started, no new participants can join, even if they have the meeting ID and password (if you have required one). In the meeting, click Participants at the bottom of your Zoom window. In the Participants pop-up, click the button that says Lock Meeting.
- Set up your own two-factor authentication: You don't have to share the actual meeting link! Generate a random Meeting ID when scheduling your event and require a password to join. Then you can share that Meeting ID on Twitter but only send the password to join via DM.
- Remove unwanted or disruptive participants: From that Participants menu, you can mouse over a participant's name, and several options will appear, including Remove. Click that to kick someone out of the meeting.
- Allow removed participants to rejoin: When you do remove someone, they can't rejoin the meeting. But you can toggle your settings to allow removed participants to rejoin, in case you boot the wrong person.
- Put 'em on hold: You can put everyone else on hold, and the attendees' video and audio connections will be disabled momentarily. Click on someone's video thumbnail and select Start Attendee On Hold to activate this feature. Click Take Off Hold in the Participants list when you're ready to have them back.

- Disable video: Hosts can turn someone’s video off. This will allow hosts to block unwanted, distracting, or inappropriate gestures on video or for that time your friend’s inside pocket is the star of the show.
- Mute participants: Hosts can mute/unmute individual participants or all of them at once. Hosts can block unwanted, distracting, or inappropriate noise from other participants. You can also enable Mute Upon Entry in your settings to keep the clamor at bay in large meetings.
- Turn off file transfer: In-meeting file transfer allows people to share files through the in-meeting chat. Toggle this off to keep the chat from getting bombarded with unsolicited pics, GIFs, memes, and other content.
- Turn off annotation: You and your attendees can doodle and mark up content together using annotations during screen share. You can disable the annotation feature in your Zoom settings to prevent people from writing all over the screens.
- Disable private chat: Zoom has in-meeting chat for everyone or participants can message each other privately. Restrict participants’ ability to chat amongst one another while your event is going on and cut back on distractions. This is really to prevent anyone from getting unwanted messages during the meeting.

This blog was updated March 31 with information about the default setting for Zoom Waiting Rooms.

Zoom has helped thousands of schools and teachers around the world quickly shift to remote virtual learning, and we want all of them to have the same productive environment as their traditional classroom settings.

Zoom comes pre-stocked with numerous security features designed to control online classrooms, prevent disruption, and help educators effectively teach remotely. Here are some best practices for securing your virtual classroom using Zoom.

Lock your virtual classroom

Did you know you can lock a Zoom session that’s already started, so that no one else can join? It’s kind of like closing the classroom door after the bell. Give students a few minutes to file in and then click Participants at the bottom of your Zoom window. In the Participants pop-up, click the button that says Lock Meeting.

How to lock your classroom

Control screen sharing

To give instructors more control over what students are seeing and prevent them from sharing random content, Zoom recently updated the default screen-sharing settings for our education users. Sharing privileges are now set to “Host Only,” so teachers by default are the only ones who can share content in class. However, if students need to share their work with the group, you can allow screen sharing in the host controls. Click the arrow next to Share Screen and then Advanced Sharing Options. Under “Who can share?” choose “Only Host” and close the window. You can also change the default sharing option to All Participants in your Zoom settings.

How to manage screen sharing

Enable the Waiting Room

The Waiting Room feature is one of the best ways to protect your Zoom virtual classroom and keep out those who aren’t supposed to be there.

When enabled, you have two options for who hits the Waiting Room before entering a class:

1. All Participants will send everyone to the virtual waiting area, where you can admit them individually or all at once.

2. Guest Participants Only allows known students to skip the Waiting Room and join but sends anyone not signed in/part of your school into the virtual waiting area.

The virtual Waiting Room can be enabled for every class (in your settings) or for individual classes at the scheduling level.

Update: Starting March 31, the Waiting Room feature will be automatically turned on by default. Visit our support page for more information on adjusting your Waiting Room settings.

How to enable the Waiting Room

Lock down the chat

Teachers can restrict the in-class chat so students cannot privately message other students. We'd recommend controlling chat access in your in-meeting toolbar controls (rather than disabling it altogether) so students can still interact with the teacher as needed.

How to control chat access

Remove a participant

If someone who's not meant to be there somehow manages to join your virtual classroom, you can easily remove them from the Participants menu. Hover over their name, and the Remove option (among other options) will appear. Click to remove them from your virtual classroom, and they won't be allowed back in.

How to remove a participant

Security options when scheduling a class

The cool thing about Zoom is that you have these and other protection options at your fingertips when scheduling a class and before you ever have to change anything in front of your students. Here are a few of the most applicable:

- Require registration: This shows you every email address of everyone who signed up to join your class and can help you evaluate who's attending.
- Use a random meeting ID: It's best practice to generate a random meeting ID for your class, so it can't be shared multiple times. This is the better alternative to using your Personal Meeting ID, which is not advised because it's basically an ongoing meeting that's always running.
- Password-protect the classroom: Create a password and share with your students via school email so only those intended to join can access a virtual classroom.
- Allow only authenticated users to join: Checking this box means only members of your school who are signed into their Zoom account can access this particular class.
- Disable join before host: Students cannot join class before the teacher joins and will see a pop-up that says, "The meeting is waiting for the host to join."
- Manage annotation: Teachers should disable participant annotation in the screen sharing controls to prevent students from annotating on a shared screen and disrupting class.

Note: For schools scheduling classes through an LMS, some of these settings might appear a little differently. Visit support.zoom.us if you need assistance.

Additionally, teachers have a couple in-meeting options to control your virtual classroom:

- Disable video: Turn off a student's video to block distracting content or inappropriate gestures while class is in session.
- Mute students: Mute/unmute individual students or all of them at once. Mute Upon Entry (in your settings) is also available to keep the clamor at bay when everyone files in.

- Attendee on-hold: An alternative to removing a user, you can momentarily disable their audio/video connections. Click on the attendee's video thumbnail and select Start Attendee On-Hold to activate.
-

Important recommendation for teachers

Teachers: We encourage you to NOT post pictures of your virtual class on social media or elsewhere online. While it's fun to share in the excitement of connecting over Zoom, we are particularly committed to protecting the privacy of K-12 users and discourage publicly posting images of students, especially minors, in a Zoom virtual classroom.

Get Zooming securely

You can also check out this video on securing your virtual classroom from the Zoom team: https://youtu.be/p1IMmOujc9c
https://blog.zoom.us/wordpress/2018/05/23/zoom-gdpr-compliance/ - GDPR guidance

NB: Please refer to MHPS Blended Learning Policy 2021. The policy was updated following the review in January 2021 and agreed by FGB, February 2021.