



Google Meet Platform protocols for Belvue

Belvue School authorises the use of the **Google Meet** (G Suite) platform to enable members of the school community to connect remotely via video link in order to attend meetings and or deliver therapy sessions.

The types of meetings permitted are as follows:

- Daily team briefings
- Meetings with parents
- Class group meetings
- Class online lessons
- Therapy sessions

The fair reason for processing information using this platform is to enable the school to carry out its public task in the education and welfare of pupils and the governance of the school during a period of closure and phased reopening due to the coronavirus pandemic.

Google Meet rely on the following fair reasons for processing (i) consent (where applicable), (ii) to perform a contract with a customer (iii) for other legitimate and business interests.

Use of and processing of personal and sensitive data (Google for Education)

Google Meet

How Google Meet keeps your video conferences protected

- With Meet, institutions can take advantage of the same secure-by-design infrastructure, built-in protection, and global network that Google uses to secure your information. Meet includes protections to safeguard student and educator privacy, including:
- Meet adheres to IETF security standards for Datagram Transport Layer Security (DTLS) and Secure Real-time Transport Protocol (SRTP).
- In Meet, all data is encrypted in transit by default between the client and Google for video meetings on a web browser, on the Android and iOS apps, and in meeting rooms with Google meeting room hardware.
- Each Meeting ID is 10 characters long, with 25 characters in the set, so it's difficult to make an unauthorized attempt to join the meeting by guessing the ID.
- To limit the attack surface and eliminate the need to push out frequent security patches, Meet works entirely in your browser. This means we do not require or ask for any plugins or software to be installed if you use Chrome, Firefox, Safari, or Microsoft Edge. On mobile, we recommend that you install the Meet app.
- *Supporting compliance requirements around regulations including COPPA, FERPA, GDPR,*





Google Meet Privacy Appliance

Google is committed to building products that protect the privacy of students and educators, and provide best-in-class security for your institution.

Customer data—The Education editions, which include Meet, do not use customer data for advertising. Google Cloud does not sell customer data to third parties. Meet does not have user attention-tracking features or software.

- **Transparency**—Google is committed to transparency about our data collection policies and practices. The [Education edition privacy notice](#) and [agreement](#) explain our contractual obligations to protect your data. We follow a rigid process for responding to [government requests](#) for customer data and we disclose information about the number and type of requests we receive from governments in the [Google Transparency Report](#).
- **Regular audits**—We undergo regular rigorous security and privacy audits for our Cloud services, including Meet.
- **Data retention**—With Google Vault, admins can [set retention policies for Meet recordings](#) stored in Google Drive. This is useful to fulfill legal obligations.
- **Smart features and personalization**—You or your users decide whether smart features in Gmail, Chat, and Meet, and personalization features in other Google products, can use data from Gmail, Chat, and Meet. You can configure these settings for users, and users can always [choose their own settings](#). Learn more about [Smart features and personalization](#).

Encryption

- All data in **Meet** is encrypted in transit by default between the client and Google for video meetings on a web browser, on the Android and iOS apps, and in meeting rooms with Google Meet hardware.
- Note: If you join a meeting by phone, audio is carried by the telephone network and might not be encrypted.

Counter-abuse measures

In **Meet**, we use a number of [counter-abuse measures](#) to keep your meetings safe. For Education and Enterprise for Education editions, we've added additional counter-abuse further.

Google Meet Security

With **Google Meet**, schools can take advantage of the same secure-by-design infrastructure, built-in protection, and global network that Google uses to secure your information and safeguard your privacy.

Privacy and compliance

- Encryption
- Counter-abuse measures
- Secure deployment, access and controls
- Incident response
- Reliability

For more details, [Google Meet Privacy and Security Centre Link](#)





How Google Meet Works

- **Required approval for external participants**—Only the meeting creator can see and approve requests to join the video meeting from participants from outside of the school's domain.
- **Improved meeting moderation controls**—Only meeting creators and calendar owners can mute or remove other participants. This ensures that instructors can't be removed or muted by student participants.
- **Protection against reusing finished meetings**—Meeting participants can't re-join nicknamed meetings once the final participant has left, unless they have meeting creation privileges to start a new meeting. This means if the instructor is the last person to leave a nicknamed meeting, students can't join again until an instructor restarts the nicknamed meeting.

Optimize security for our school staff must do the following:

- **Prevent students and others from becoming a host or entering meeting before host**
 - Disable the quick access in settings before the meeting. This has to be done for every meeting you are hosting.
- **Prevent students from reusing class meetings**—
 - To make sure students don't re-join a class meeting/online lesson after it has ended, use nicknamed meetings.
 - **Use Meet via Google Classroom**
 - **Do not start a meeting from a Google Calendar event.**
- Even if you reuse the same nickname, participants **will not be able to re-join nicknamed meetings** after the **final participant has left** and the 10-digit meeting code will no longer work.
 1. **Ensure all students have left the meeting before you end the meeting.**
 2. **There is a 30 second delay ensure you **enter again before 30 seconds expire** to check students have left and not re-entered meeting.**
- To create a nicknamed meeting, use one of the following methods:
 1. Use a short link like g.co/meet/nickname.
 2. Go to meet.google.com or the Meet mobile apps and enter a meeting nickname in the "Join or start a meeting" field.
 3. Use the Meet code automatically generated by Google Classroom
 4. Add or remove people from a Google Meet video call

You can add people to a video meeting in Google Meet before or after the meeting starts. You can also remove people during a video meeting.

1. Some people need to request permission before they can join the video meeting. For details, go to Join a video meeting.





To minimise the possibility or impact of a meeting being hacked staff must do the following:

To minimise the possibility or impact of a meeting being hacked staff must do the following:

- A link is automatically given when starting a meeting
- **Use a nickname** for all meetings
- Using a nickname stops students from joining a Meeting without the teacher.
- **Securing your host privileges** host controls in settings: **Disable Quick Access:** Allowing host to join first, only people invited can join without being asked, everyone else must be asked to join, even when dialing in, people cannot join anonymously, only host can dial out meeting.
- **Check all attendees' names** before accepting them into the meeting (And those outside of Belvue school account).
- Ensure all **attendees enable their video to identify themselves** to you
- **Familiarise** yourself in advance with **how to remove a person** from a meeting in case you ever needed to use this
- **Chat option:** There is only one option and everyone can see the chats (Explain good practice and protocols when using the message option – no offensive messages accepted)
- **Disable chat option:** This can be done in settings
- **Disable 'share screen'** so pupils do not have access to this function to minimise the risk of offensive material Do this in advance before they enter Meet.
- When everyone invited has joined the meeting you can still monitor those who want to join
- Make sure **all attendees have left meeting** then end as host

To minimise the risk or potential for significant harm through a data breach, the following protocols must be adopted:

Staff daily briefings - These meetings will be sharing information of an operational nature. Only first names of staff or pupils should be used during the meetings. Where possible all the above security settings should be adopted however the content of these meetings are not confidential and therefore low risk. Confidential or sensitive documents should not be shared on the share screen function.

Meetings with parents for annual reviews/family workers meetings – These meetings will consist of discussions of a personal and sensitive nature regarding the young people and their families. All the above security settings must be adopted particularly with regards to a password to access the meeting. It would not be advisable to share confidential documents on the screen; these should be sent to the parents ahead of the meeting in the usual secure manner – either by egress or a password protected document. Any personal identifiers such as addresses should not be read out during the call.





To minimise the possibility or impact of a meeting being hacked staff must do the following:

Class group meetings/Online lessons – These classes meetings/online lessons are critical to pupil wellbeing and learning during school closure and may include pupils sharing their personal experiences together. Confidential matters are not discussed though. For safeguarding purposes all class meetings/lessons must be hosted by two staff members. The meeting/online lessons must not start until both staff members are online first. The waiting room function must be used to hold pupils in until both staff are ready to commence. Both staff members must be in attendance at all times and should not leave the meeting/online lesson. If an emergency arises the meeting should be stopped and reconvened at a later time. Pupils should not disclose any personal identifiers during the meeting such as addresses. Only first names should be used and students must blur their background when having an online lesson/meeting.

Combined Teaching students online and in class – Ensure students in the classroom are not in the view of the camera when delivering combined lessons. A TA/Support staff will support students in the class and another TA/Support staff will monitor and be present with the students who are online.

If a medical emergency takes place in class the TA/other staff member who is online with the students will ask the students to leave the lesson ensuring students do not reenter the Meet room.

If a medical emergency takes place when student is online the teacher who is online with the students will ask the students to leave the lesson ensuring students do not reenter the Meet room whilst the TA makes contact with the family to alert them to the situation or calls an ambulance in an emergency. The meet room will need to remain open to the sick child until the situation has been resolved.

Therapy sessions- At Belvue school we consider these sessions essential to the well being of our pupils particularly during school closure where the pupils may require more support. During these sessions confidential information will be shared and discussed with the therapists, which will remain confidential outside of that forum, as it is when the sessions take place in the building. Due to the nature of these sessions, only the therapist and the pupil or pupils will be in the meeting.

All sessions - Online contact with pupils MUST only be during school hours.





To minimise the possibility or impact of a meeting being hacked staff must do the following:

Screen Sharing – Staff may wish for pupils to share work or pictures during meetings in the spirit of collaboration. Staff should be mindful that screen shots can be taken during Google Meet without your knowledge and that any photos shared are subject to consent from the individuals concerned. Pupils should also be advised that taking screen shots of the meeting is not allowed and ascertain their understanding and consensus of this. It is not appropriate to share confidential documents using the Google Meet platform. Staff should be extremely careful of sharing anything on their computer screen as they could inadvertently share something confidential they have open. Backgrounds and photos on school equipment should be professional and in line with the code of conduct expectations at all times.

Recording of Google Meet (Disabled from Admin Side)– Due to the increased risks of security around recording and storing using Google Meet Belvue staff are not allowed to record meetings. By default only Google Meet hosts can record meetings and staff must not record or give permission and access for anyone else to record the meetings.

Professional behaviour and conduct – Belvue staff are allowed to attend these meetings remotely and in their own home. However staff are representing the school and need to ensure they are adhering to the code of conduct and not acting in a manner that could affect the schools reputation.

Staff must therefore ensure the following:

- Meetings with parents must be conducted with the upmost consideration for confidentiality. You should be in a private room away from other family members
- Be mindful of your professional presentation to parents and pupils; dress and setting should be appropriate and not distracting
- You should have a secure internet connection, i.e. your router should be locked with a password so that other people in the vicinity cannot join your network and hack the meeting
- You have the option to blur your background when holding a meeting from home

Invitations and consents – All parents who are scheduled to have a Google Meet must be emailed the script in Appendix 1 to provide them with information about the platform, its privacy policy, and our protocols to keep the meeting secure. The parent should email back confirming they have read the information and are happy to consent to the meeting on this basis.

All parents must also be emailed the script/timetable in Appendix 2 to confirm the protocols for pupil's weekly class group meetings/lessons and or therapy sessions. Parents to sign and return slip to Class/VT teacher confirming they have read the information.



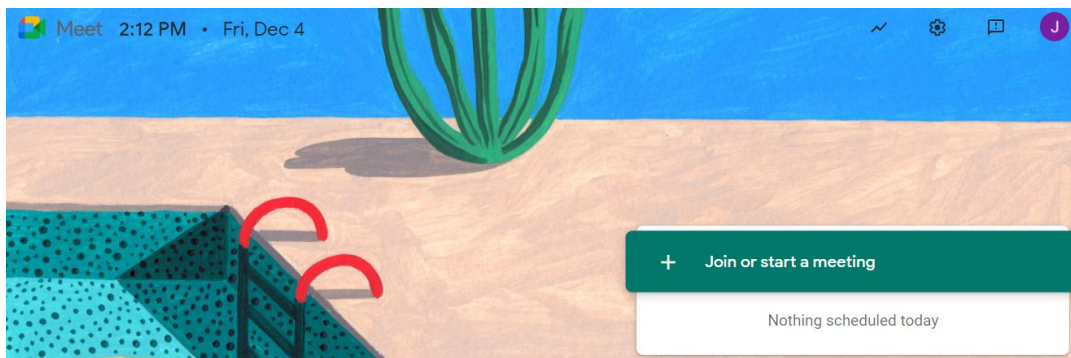


How to manage your Google Meet settings in accordance with Belvue Protocol

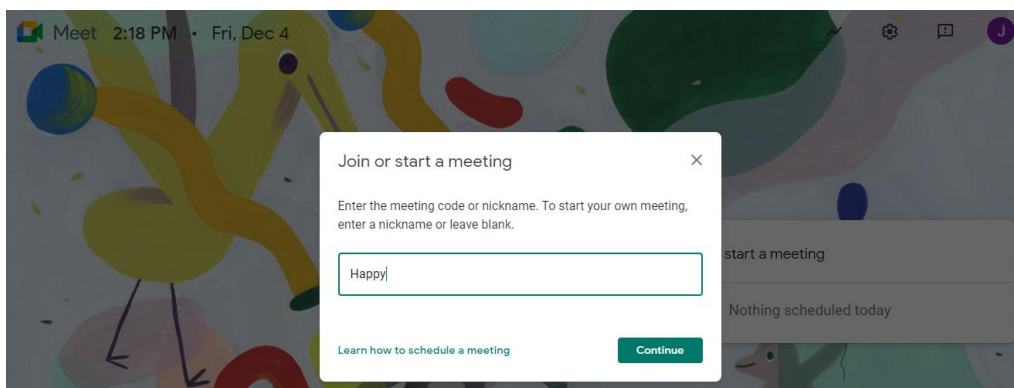
Optimize security for our school staff must do the following:

1. Prevent students from reusing class meetings—[use nicknamed meetings](#).

Join or start a meeting via Meet App



Creating a nickname



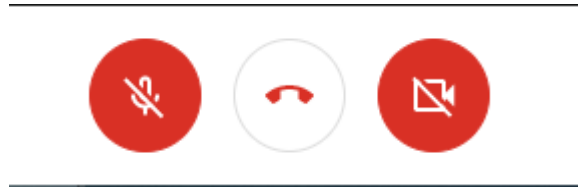
Even if you reuse the same nickname, participants **will not be able to re-join nicknamed meetings** after the **final participant has left** and the 10-digit meeting code will no longer work.





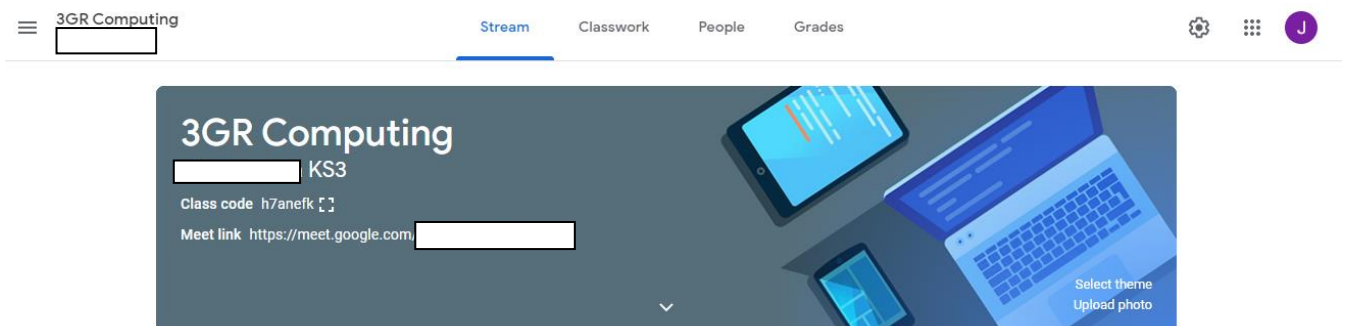
How to manage you Google Meet settings in accordance with Belvue Protocol

2. Ending a Meet call




- Ensure all students have left the meeting before you end the meeting

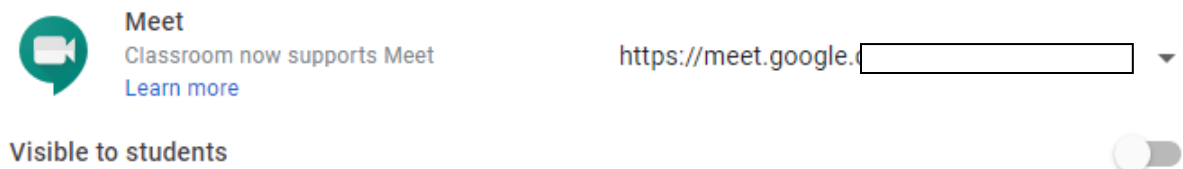
3. Using a Meet code automatically generated by Google Classroom



- Ensure after use the Meet link is disabled

Go to settings (Top right of main page) 

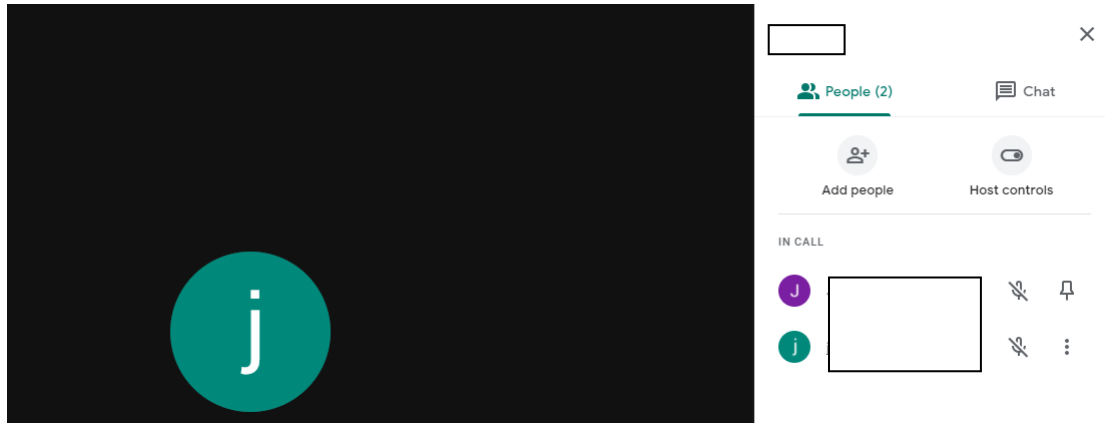
Scroll down and disable



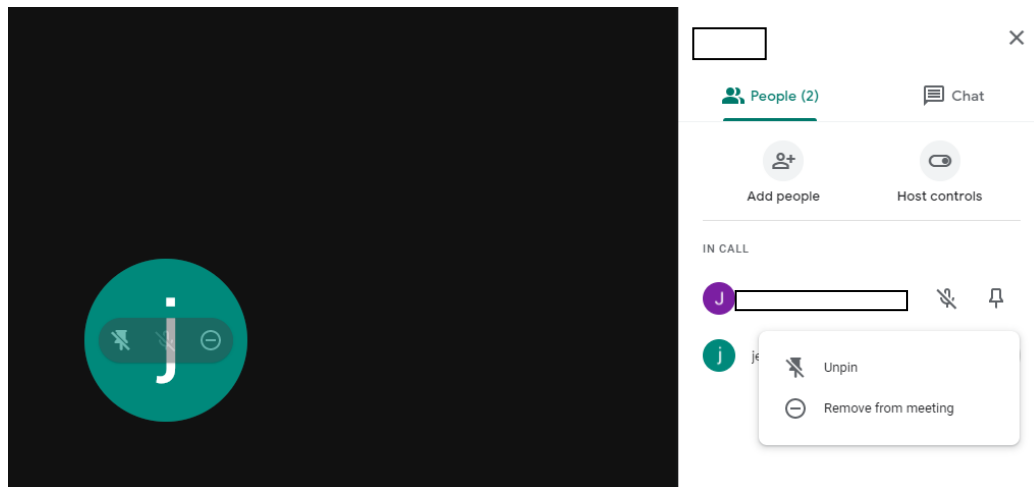


How to manage you Google Meet settings in accordance with Belvue Protocol

4. Removing participants from Google Meet



Go to participant you wish to remove and click on the 3 dots

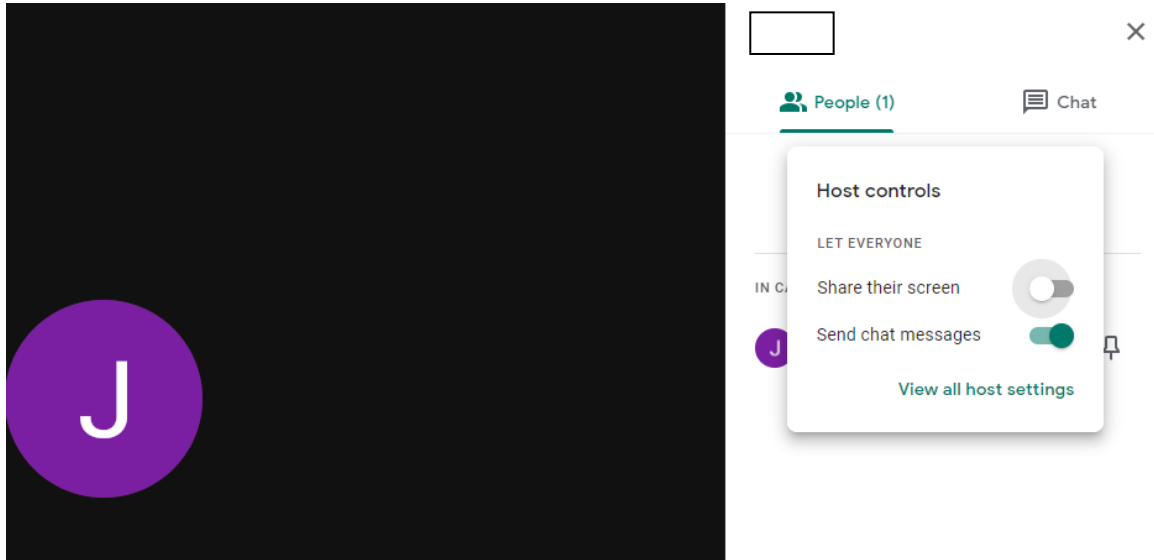


You then have the option to remove participant from meeting

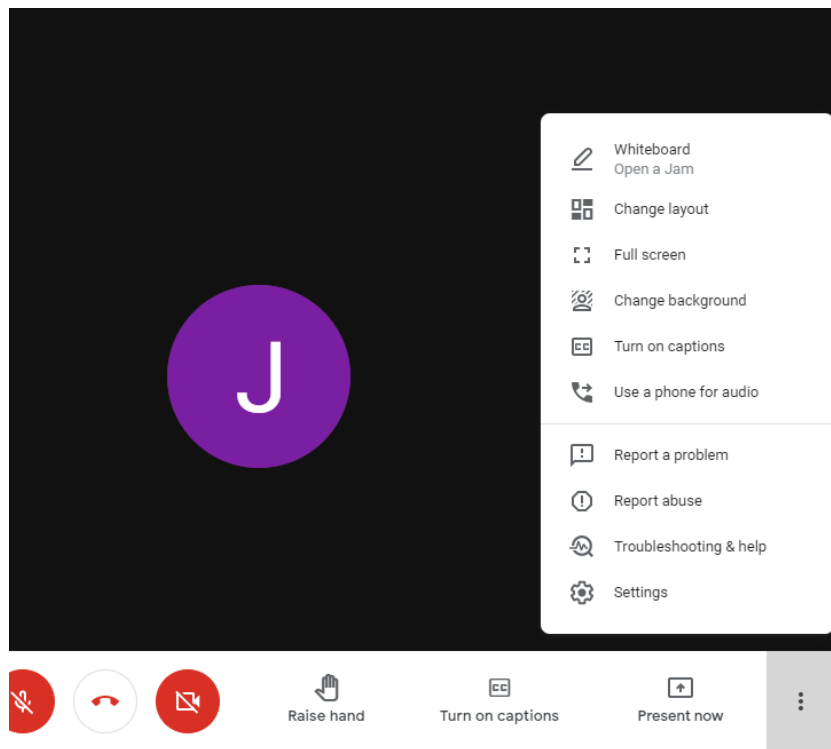


How to manage you Google Meet settings in accordance with Belvue Protocol

5. Other host controls



Short cut for host controls (Top right) click show everyone-people)



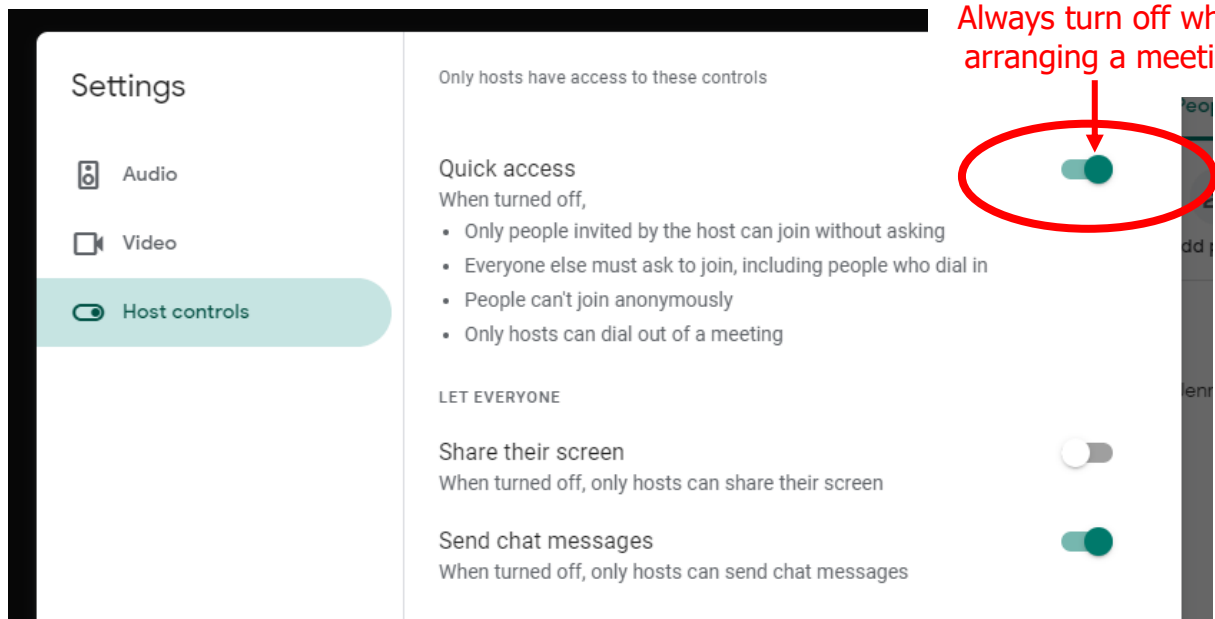
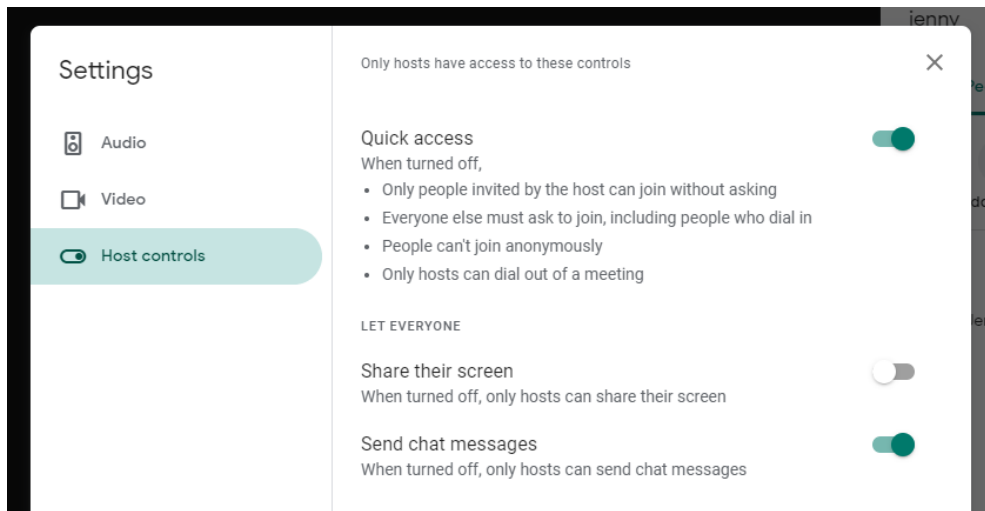
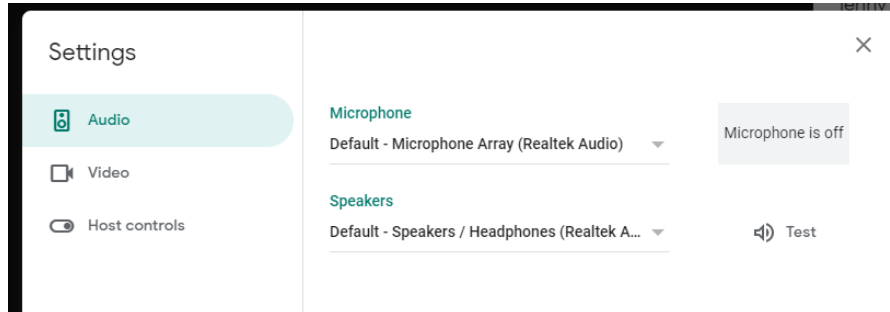
All settings for host (Bottom bar, 3 dots, right click)





How to manage your Google Meet settings in accordance with Belvue Protocol

6. All settings





Appendix 1.

Dear _____

Use of Google Meet Platform for parents meetings

You will shortly receive a meeting invitation for your child's annual review.

We will be using the Google Meet video platform to host this meeting.

We would like to refer you to the [Google Meet privacy policy](#)

I can also confirm the following school protocols to preserve the confidentiality and security of the meeting/online lesson:

- The meeting/online lesson will be password protected and you will need to use the password to access it
- You do not need to set up an account to access the meeting/online lesson and the only information you need to provide Google Meet with is an onscreen name
- The meeting/online lesson settings will be 3rd party encrypted and on a password protected account
- All staff will use a password protected secure internet connection, we also ask parents to ensure that their internet routers are on a secure password protected connection
- We will not share any confidential documents with you on the screen, any documents will be emailed or posted to you securely ahead of the meeting/online lesson
- We will not record any meetings/online lessons
- We will not give access to the meeting to any other parties
- We will not ask you to provide any personal identifiers such as address over the video meeting and we will not do this either.

Please can you reply confirming that you have read the Google Meet policy and school protocols for security and are happy for the meeting to go ahead? We can then schedule in the meeting at the agreed date and time.

Yours sincerely



Appendix 2

Dear _____

Class group using Google Meet for video class meetings/online lessons

I will be setting up regular class lessons using the Google Meet video meeting platform.

This will be a wonderful opportunity for the pupils to see each other online and stay connected together whilst the physical school site remains on a restricted service.

I would like to refer you to the [Google Meet privacy policy](#)

I can also confirm the following school protocols to preserve the confidentiality and security of the meeting:

- The meeting/online lesson will be password protected and your child will use their personal school login and password to access it
- You do not need to set up an account to access the meeting/online lesson and the only information you need to provide Google Meet with is an onscreen name
- The meeting settings will be 3rd party encrypted and on a password protected account
- All staff will use a password protected secure internet connection, we also ask parents to ensure that their internet routers are on a secure password protected connection
- We will not share any confidential documents with you on the screen, any documents will be emailed or posted to you securely ahead of the meeting
- We will not record any meetings/online lessons
- We will not give access to the meeting to any other parties
- We will not ask your child to provide any personal identifiers such as address over the video meeting and we will not do this either
- The meeting/online lesson will be hosted by two Belvue staff members at all times and they both be online first before accepting pupils into the meeting
- Unknown persons attempting to gain access to the meeting will be refused
- Meetings/online lessons will be 'locked' once all expected attendees have arrived
- Pupils are expected to enable their videos to be visible on screen however if you are concerned about others seeing you on the online lesson you have the option of turning off the camera
- Pupils are expected to blur their background
- The public and private 'chat' functions will be disabled
- Some screen sharing may take place for work and pictures, subject to the consent of the individuals concerned
- Pupils are advised that they are not allowed to screen shot the video call at any time or record the sessions using a device, pupils found to be breaching this may be banned from future meetings
- If behaving inappropriately you will be muted or removed from the meeting/online lesson

Please can you sign and return slip confirming that you have read the Google Meet policy and school protocols for your child to attend the online meetings/online lessons.



Appendix 2

Class group using Google Meet for video class meetings/online lessons

RETURN THIS PART ONLY to: admin@belvue.ealing.sch.uk

Name of pupil Click here to enter text. Class/VT Click here to enter text.

This is to confirm that I have read the Google Meet policy and school protocols for my child to attend the online class meetings/ lessons.

Signed Click here to enter text. Name Click here to enter text. Date Click here to enter text.
(Parent/Carer)



Appendix 3

Dear _____

Therapy sessions using Google Meet for video/online therapy

The therapists at Belvue school will be setting up regular sessions using the Google Meet video meeting platform.

This will be a wonderful opportunity for the pupils to continue accessing this precious support even through these difficult times whilst the physical school site remains on a restricted service.

I would like to refer you to the [Google Meet privacy policy](#)

I can also confirm the following school protocols to preserve the confidentiality and security of the meeting:

- The session will be password protected and your child will use their personal school login and password to access it
- You do not need to set up an account to access the meeting/online session and the only information you need to provide Google Meet with is an onscreen name
- The meeting settings will be 3rd party encrypted and on a password protected account
- All staff will use a password protected secure internet connection, we also ask parents to ensure that their internet routers are on a secure password protected connection
- We will not share any confidential documents with you on the screen, any documents will be emailed or posted to you securely ahead of the meeting if required.
- We will not record any meetings/online lessons
- We will not give access to the meeting to any other parties
- We will not ask your child to provide any personal identifiers such as address over the video meeting and we will not do this either
- The meeting/online session will be hosted by a Belvue staff member/therapist Unknown persons attempting to gain access to the meeting will be refused
- Meetings/online session will be 'locked' once all expected attendees have arrived if there is more than one.
- Pupils are expected to enable their videos to be visible on screen
- The public and private 'chat' functions will be disabled
- Some screen sharing may take place for work and pictures, subject to the consent of the individuals concerned
- Pupils are advised that they are not allowed to screen shot the video call at any time, pupils found to be breaching this may be banned from future meetings

Please can you sign and return slip confirming that you have read the Google Meet policy and school protocols for your child to attend the online meetings/online lessons.

Yours sincerely



Appendix 3

Therapy sessions using Google Meet for video/online therapy

RETURN THIS PART ONLY to school office : admin@belvue.ealing.sch.uk/therapist Lead:
marinap@belvue.ealing.sch.uk

Name of pupil Click here to enter text. Therapy Click here to enter text.

This is to confirm that I have read the Google Meet policy and school protocols for my child to attend the online class meetings/ lessons.

Signed Click here to enter text. Name Click here to enter text. Date Click here to enter text.
(Parent/Carer)