# BHES

*“Online safety policy”*

Note: in this policy reference to governing body or governors refers to the management committee and its members.
Where contextually appropriate for school read service.

**Date adopted: 16/12/2020**

## HISTORY OF POLICY CHANGES

| Date | Page | Details of Change |
|---|---|---|
| May 2021 | All | Reviewed – no change |
| April 2022 | | Removal of Meriton logo |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# Contents



## 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for head teachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education

Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

# 3. Roles and responsibilities

## 3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the head teacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 4)

## 3.2 The head teacher

The head teacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

## 3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the head teacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the head teacher and/or governing board
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

## 3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a regular basis as set out by Bristol City Council
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

## 3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (https://forms.gle/wYZ9aea5sM9eDpSj6), and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

## 3.6 Parents

Parents are expected to:

- Notify a member of staff or the head teacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (provided via google form during initial induction)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

## 3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

## 4. Educating pupils about online safety

PLEASE NOTE:

Students at BHES receive short term input to enable them to return to their on roll school, we do not always deliver all aspects of the school curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

*By the **end of primary school**, pupils will know:*

- *That people sometimes behave differently online, including by pretending to be someone they are not.*
- *That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous*
- *The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them*
- *How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met*
- *How information and data is shared and used online*
- *How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know*

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

*By the **end of secondary school**, they will know:*

- *Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online*

- *About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online*
- *Not to provide material to others that they would not want shared further and not to share personal material which is sent to them*
- *What to do and where to get support to report material or manage issues online*
- *The impact of viewing harmful content*
- *That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners*
- *That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail*
- *How information and data is generated, collected, shared and used online*
- *How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours*

The safe use of social media and the internet will also be covered in other subjects where relevant.

# 5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Facebook Parent group. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head teacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the head teacher.

# 6. Cyber-bullying

## 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

## 6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

### 6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

**Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.**

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

## 7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

During induction the Acceptable Use Agreement is completed via a Google form:

Classes students - https://forms.gle/1gQjD7kGiccE7oR9A

1:1 students - https://forms.gle/43AP1vJFoUaz1Eot7

Staff will complete a new agreement each year:

Staff, governing body, volunteers and visitors - https://forms.gle/AofMdj47i1cswfQs5

## 8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

## 9. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely for work activities.

## 10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

For further information see Appendix 2.

## 11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

## 12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety, this can be found on CPOMS.

This policy will be reviewed every yearly by the DSL. At every review, the policy will be shared with the governing board.

## 13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

# Appendix 1: online safety training needs – self audit for staff

| ONLINE SAFETY TRAINING NEEDS AUDIT | |
|---|---|
| **Name of staff member/volunteer:** | **Date**: |
| **Question** | **Yes/No (add comments if necessary)** |
| Do you know the name of the person who has lead responsibility for online safety in school? | |
| Do you know what you must do if a pupil approaches you with a concern or issue? | |
| Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors? | |
| Are you familiar with the school's acceptable use agreement for pupils and parents? | |
| Do you regularly change your password for accessing the school's ICT systems? | |
| Are you familiar with the school's approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? | |

# Appendix 2: Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from BHES and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school/academy context, either because of the age of the users or the nature of those activities.

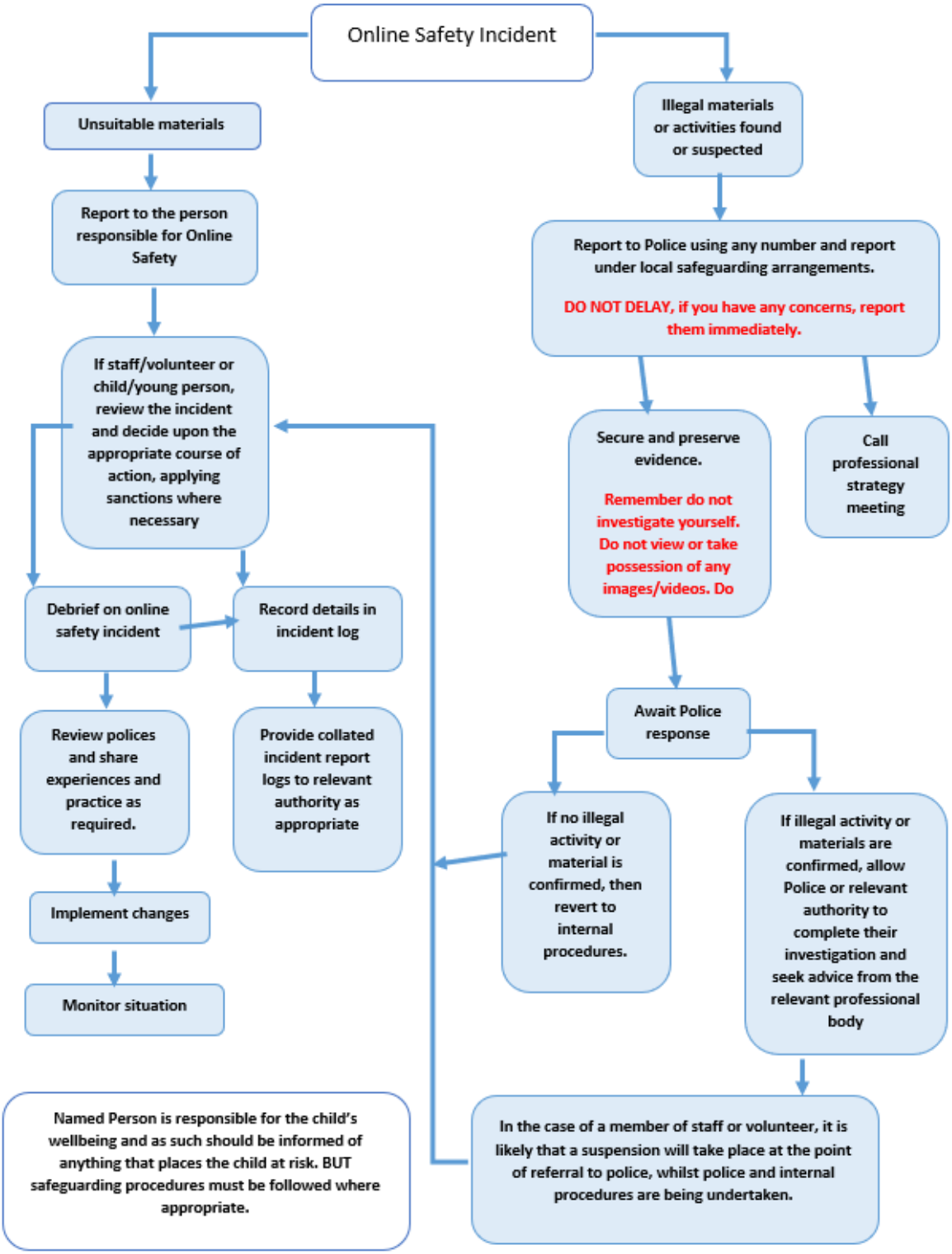
BHES believes that the activities referred to in the following section would be inappropriate in a BHES context and that users, as defined below, should not engage in these activities in/or outside the school/academy when using school/academy equipment or systems. The school/academy policy restricts usage as follows:

| User Actions | | Acceptable | Acceptable at certain times | Acceptable for nominated users | Unacceptable | Unacceptable and illegal |
|---|---|---|---|---|---|---|
| Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: | Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978<br><br>N.B. Schools/academies should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges | | | | | X |
| | Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003. | | | | | X |
| | Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008 | | | | | X |
| | Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986 | | | | | X |
| | Pornography | | | | X | |
| | Promotion of any kind of discrimination | | | | X | |
| | threatening behaviour, including promotion of physical violence or mental harm | | | | X | |
| | Promotion of extremism or terrorism | | | | X | |
| | Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute | | | | X | |

| | | | | | |
|---|---|---|---|---|---|
| Activities that might be classed as cyber-crime under the Computer Misuse Act:<br>• Gaining unauthorised access to school networks, data and files, through the use of computers/devices<br>• Creating or propagating computer viruses or other harmful files<br>• Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)<br>• Disable/Impair/Disrupt network functionality through the use of computers/devices<br>• Using penetration testing equipment (without relevant permission)<br><br>N.B. BHES will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information here | | | | | X |
| Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy | | | | X | |
| Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords) | | | | X | |
| Unfair usage (downloading/uploading large files that hinders others in their use of the internet) | | | | X | |
| Using school systems to run a private business | | | | X | |
| Infringing copyright | | | | X | |

## Appendix 3: Illegal Incidents

If there is any suspicion that the website(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



# Appendix 4: Remote learning: safeguarding pupils and staff

**The following information is from The Key as advice to schools**

**Use school channels to communicate**

As always, staff shouldn't communicate with parents or pupils outside school channels (e.g., they shouldn't talk to parents using their personal Facebook accounts, or contact pupils using their personal email addresses or phone numbers).

If you have expectations with parents already about contacting staff and when they'll get replies, remind them about these. Similarly, remind staff about any expectations you've already set in your code of conduct for communicating with pupils and parents, and staff-pupil relationships.

**What to do in different scenarios**

We've based these scenarios on using open Google Drives, the features of G Suite for Education (e.g. Google Classroom and Google Meet), the features of Office 365 Education (e.g. Microsoft Teams) and YouTube, as these are among the most commonly-used platforms at the moment.

- **If teachers are uploading resources to an *open* Google Drive**

Make sure there's nothing that can identify pupils in the resources, like their names or comments addressed specifically to them, as anyone with the link can view what's in an open Drive.

Note: if you're using a Google Drive as part of G Suite for Education, you don't need to worry about this. By default, your school's Google Drive will only be visible to users in your school.

- **If you're using Google Classroom to set work and communicate**

Decide:

Whether you'll allow pupils to post and comment in the communication 'Stream', or disable this function for them (see below)

What they can talk about in posts and comments, if allowed to

(If you disable pupil comments in the 'Stream', pupils will still be able to respond to feedback from their teacher on work they've handed in – they just won't be able to post on the 'Stream' page.)

To disable pupil comments in the 'Stream':

1. Open your class in Google Classroom
2. Click 'Settings' (the cog icon)
3. Scroll down to 'General'
4. Click the drop-down option to the right of 'Stream' and select 'Only teachers can post or comment'
5. Click 'Save'

If you allow pupils to comment, tell them they should only talk about school work in the 'Stream' and that you may 'mute' them, i.e. stop them from posting or commenting (see below), if they post anything that's inappropriate or bullying in nature.

Give parents the chance to opt out of their child posting in the 'Stream' too. If they opt their child out, mute them.

To 'mute' a pupil:

1. Click on a class in Google Classroom
2. Click 'People'
3. Next to the pupil you want to mute, check the box
4. Click 'Actions' > 'Mute'
5. Click 'Mute' again to confirm

To delete inappropriate or bullying posts or comments (you'll still be able to view them if you need to use them as evidence – see below):

1. Go to the class
2. Find the post or comment you want to delete
3. Click 'More' (the 3 dots) > 'Delete'
4. Click 'Delete' again to confirm

To view deleted posts and comments:

1. Go to the class
2. Click 'Settings' (the cog icon)
3. Next to 'Show deleted items', click 'Show' to toggle on
4. Hide the deleted items again by clicking 'Hide' to toggle off
5. Click 'Save' to save your changes and return to the 'Stream' page

**If you're using Google Chat and Google Meet**

Decide whether you'll let pupils communicate in Google Chat (previously called Google Hangouts). Like any chat function, it could lead to bullying, or be a distraction from learning.

To turn off Google Chat, you need to be an administrator. From the Admin Console Homepage, go to:

1. Apps > G Suite > Hangouts Chat
2. Click 'Service status'
3. To turn chat off for everyone, click 'Off for everyone'
4. Click 'Save'

This will turn off the chat function for everyone – staff and pupils. If you just want to turn it off for pupils, follow the more intricate steps here (particularly step 5).

Tell teachers to:

- Sit against a neutral background
- Avoid recording in their bedroom where possible (if that's not possible, use a neutral background)
- Dress like they would for school – no pyjamas!
- Double check that any other tabs they have open in their browser would be appropriate for a child to see, if they're sharing their screen
- Use professional language

Ask pupils to also be in a shared space in their house, rather than in their bedroom. No pyjamas for pupils either! Alternatively, you could ask them to turn their cameras off.

Ask parents who'll also be there to be mindful that other children might see or hear them and anything in the background.

Make a recording so there's something to go back to later on if you need to, and keep a log of who's doing video calls and when. Check that parents are happy with you making recordings first – tell them it's for school records only.

To record in Google Meet:

1. In the meeting, click 'More' (the 3 dots) > 'Record meeting'
2. Wait for the recording to start
3. When you finish, click 'More' > 'Stop recording'
4. Click 'Stop recording' again to confirm
5. Wait for the recording file to be generated and saved to the Meet Recordings folder. The meeting organiser and the person who started the recording will also get an email with the recording link

(You'll need to be using the computer version of Meet to record.)

**If you're using Google Meet for live streams**

Tell teachers to:

- Sit against a neutral background
- Avoid recording in their bedroom if they can (if that's not possible, use a neutral background)
- Dress like they would for school – no pyjamas!
- Double check that any other tabs they have open in their browser would be appropriate for a child to see, if they're sharing their screen
- Use professional language

Record live streams so there's something to go back to later on if you need to, and keep a log of who's doing live streams and when.

In 'view-only' Google live streams, pupils will be automatically muted and won't be visible, so you don't need to worry about what other adults in their homes might do that gets caught on camera.

If you schedule meetings in Google Calendar or Gmail, pupils won't be able to re-join once the final attendee has left. This means pupils won't be able to re-join for their own private calls.

You might still want to ask for pupils to be on mute with webcams off, to cut risks. Otherwise, no pyjamas for pupils either, and ask parents to be mindful of what they say and do in the background.

To record in Google Meet:

1. In the meeting, click 'More' (the 3 dots) > 'Record meeting'
2. Wait for the recording to start
3. When you finish, click 'More' > 'Stop recording'
4. Click 'Stop recording' again to confirm

5. Wait for the recording file to be generated and saved to the Meet Recordings folder. The meeting organiser and the person who started the recording will also get an email with the recording link

(You'll need to be using the computer version of Meet to record.)

**If teachers are phoning pupils**

Tell them to:

- Do this through parents' phones only (unless this itself poses a safeguarding risk), particularly in primary school, and in all cases make sure parents are aware and agree
- Call in school hours as much as possible
- Make sure someone else at school is aware, and keep a record of the date and time of each call
- Have a parent there at the child's end, and have the phone on speaker phone
- Either use an app like 3CX that will route calls through your school's number rather than their own, or block their number so parents don't see it. (Give parents a heads-up of what time you'll be calling if you're blocking numbers, so they're more likely to pick up.) Please note, the link to another product here isn't an endorsement from The Key
- If possible, have another member of staff on the call. If this isn't possible, record the call, with parents' permission. Explain you're recording for school records only

If teachers are using video calling, take the same steps as above.