



WeST Guidance on Safeguarding Remote Learning During Coronavirus

Purpose

This document should be used alongside existing Safeguarding, Staff Code of Conduct, Advice on Social Media Use, e-Safety and ICT Acceptable Use Policies and WeST Guidance on remote learning to ensure that all staff, pupils and parents are aware of how to harness the benefits of remote learning (i.e. learning through devices connected to the internet) as safely as possible.

Useful Websites

Technology and its use to support remote learning is rapidly developing. Any written policy is likely to become out of date quite rapidly. As such, Westcountry Schools Trust recognises that the core team, individual school staff and in turn pupils and parents/carers may need to refer to online sources of guidance which are more likely to be kept up to date.

At the time of writing the following websites were deemed to be 'trusted' sources of such advice. They were used to compile this summary and it is hoped they will be cross-referenced by readers of this guidance in the future as a source of current information.

[DfE Guidance on Safeguarding and Remote Education](#)

[NSPCC Advice on Remote Teaching](#)

[Advice from UK Safer Internet Centre](#)

Key Principles for Staff

1. As far as possible staff should use school devices and internet connections to deliver remote learning.
2. If delivering remote learning from home staff should use school devices as far as possible. WeST schools will take reasonable steps to ensure all staff are provided with suitable devices. However, WeST recognises that this will not be possible in all cases, and to 'blanket ban' the use of personal staff laptops etc. to deliver remote learning could be detrimental to the quality of education offered. Therefore, staff may use their own devices, if they are willing to do so, and have no other alternative. In these circumstances they should take extra care to consider e-safety principles when delivering remote learning. Pupil data **must not** be saved to personal devices.
3. Staff **must** only use their work email to communicate with pupils and parents/carers. Under no circumstances should staff communicate with pupils or parents/carers using personal email addresses or social media accounts.
4. Staff should use the locally agreed software to deliver remote learning. In most WeST schools this will be the Microsoft 365 suite, but some will use the Google platform. In either case staff **must** use their school 'username' (typically their school email) not a personal account.
5. As far as possible telephone calls to support remote learning or pupil welfare should be made using school devices. WeST recognises that not all staff will have access to a school mobile 'phone and there will be occasions when contact with a pupil and/or parent/carer is necessary, e.g. safeguarding or welfare checks. Under such circumstances staff should take steps to hide their phone number/caller ID before making a call.
6. When delivering remote learning in which they will be visible staff should consider carefully the location they use, their dress and their device settings. For example, staff:
 - a. **must** dress appropriately in accordance with the Staff Code of Conduct;
 - b. should not deliver remote learning from bedrooms (if there is no alternative staff should discuss this with their Headteacher / DSL and a note of the decision made should be recorded);
 - c. choose a 'quiet' location in their house where it is unlikely that other household occupants can be seen/heard in the background;

- d. brief other household occupants that they are delivering remote learning and that as such they should not be disturbed, except in an emergency;
 - e. should give due consideration to the background that will be visible if using a webcam and, where possible, use appropriate 'background effects' to mask details of their home location;
 - f. be careful if 'screen sharing' that no other, unsuitable content is visible elsewhere on the screen outside of the main window intended to be viewed;
7. In addition to the above if conducting 'live lessons' staff:
- a. **Must** ensure that these are recorded, and that the recording is stored on an approved server (e.g. if using MS Teams the recording would be saved via MS Stream to a secure location within the school's Microsoft 'ecosystem');
 - b. Should explain to pupils how the lesson will be conducted and remind them to behave respectfully at all times (as if in school);
 - c. Should establish and maintain clear routines regarding participation from pupils. For example,
 - i. they should instruct them in the appropriate use of the 'mute/unmute' facility on the platform being used
 - ii. explain how questions will be asked and answered
 - iii. consider how functions such as 'chat', 'Q&A' and 'hands up' on platforms such as MS Teams and Google Meet will be used.

***NB** - WeST recognises that the wide variety of staff experience and learning scenarios means that it is not prudent to recommend a blanket approach to how staff/pupils use these software facilities. Staff should follow local guidance and seek clarification through their usual line management routes if they have queries.*

Key Principles for Pupils

Individual schools should consider the most appropriate mechanism by which to ensure as far as possible pupils, and their parent/carers, are aware of and follow these principles. Schools should modify, as appropriate, the language in the statements below to take into account the age of pupils and those with SEND.

Pupils should:

1. only use school email addresses to contact staff;
2. only use their school 'usernames' to access any internet-based learning platforms being delivered by staff;
3. **not** share their username and/or password for internet platforms;
4. as far as possible, engage in remote learning in a shared space, such as a kitchen or living room. They should avoid using individual bedrooms.
5. dress appropriately, e.g. they should not wear pyjamas or 'revealing' clothes (a benchmark for this is what the school would normally allow on a non-uniform or 'Mufti' day);
6. sit against a neutral background and be mindful of what others might see behind them;
7. where possible, be taught the benefits of using appropriate 'background effects' to mask details of their home and be encouraged to use these;
8. if considered vulnerable, e.g. due to age or other circumstance, receive remote learning with a trusted adult in the vicinity;
9. behave as if they were in a classroom at school, following the school's general behaviour expectations and specific instructions from the member of staff delivering the remote learning.

Risk Assessment for using Microsoft Teams – Dunstone Primary – January 2021



Activity/Process	Identified Risks	Group (who) affected	Risk Level	Treatment to reduce or eliminate risk	Risk Level
Teacher/Pupil group sessions via Teams	Pupils could say or do something inappropriate on the session.	Pupils/Parents	moderate	At the beginning of each session an adult at home waves to the camera indicating they give permission, then leave the room. At the beginning of the year parents and pupils agree to the guidelines regarding online communication. The consequences to this are being blocked if they say or do something inappropriate (similar to a class charter). Prepare a script for staff to read before the session to discourage inappropriate behaviours and remind children and parents of the agreement. Pupils can be ejected from a meeting if they are misbehaving and would be held in the lobby before they could rejoin.	low
	Teachers delivering sessions from home showing their home environment in the background could present a Safeguarding risk by identifying personal effects or home address.	Teachers	low	Teachers will be instructed to change the background setting with MS teams to a predefined background thus removing the background of their home environment. Lessons to be delivered from the school environment, where possible. If teachers cannot change the background, ensure a blank background at home.	low
	Teachers delivering sessions from home could expose their own children if they are picked up via audio or video on the session.	Teachers	moderate	Live sessions should be undertaken from school where possible. A sign or notice to be placed on the door of the classroom where lessons are being presented to inform staff and pupils that an event is being undertaken. If live lessons are carried out at home in agreement with the Headteacher, the teacher must take appropriate steps where practical to ensure they remain uninterrupted by other members of the of the household during the lesson.	low
	Teachers delivering sessions from home or at school could be party to a disclosure from an individual child via a group video session.	Teachers	moderate	Children are reminded at the beginning of any video session that this is a lesson and any discussions about home life can be done at a different time. Teachers have been instructed that if a child is to disclose something of a personal nature, or teachers can visually see or hear something that they would consider is putting the child at risk, they immediately end the session with the wider group. Depending on the nature of the interruption the meeting can be placed on hold, disabling the audio and video capabilities within the	low

				meeting for all attendees. Any disclosures must be recorded on CPOMS	
	Pupils can record the Teams sessions and distribute the content	Teachers	high	The record feature has been turned off for pupil accounts.	low
	Pupils or Parents utilise the features (video, audio, chat) of a scheduled meeting before or after the event to discuss or share inappropriate content.	Pupils	moderate	Teachers can eject any pupil attendee in the instance of such an occurrence	low
	Pupils use the features of Teams in an ad-hoc manner with other pupils without the chairing or control from a Teacher, potentially creating a safeguarding issue	Pupils	high	Staff set the meeting options on ALL meetings, including any historic or future scheduled meetings, so that pupils can only enter meetings via the lobby and the teacher has the control to admit them in.	moderate
	School staff share sensitive information to the wrong group chat or channel in Teams which is visible to pupils.	Pupils/parents	moderate	Once identified, any inappropriate content can be deleted from a channel in Teams. Other methods e.g. e-mail can be retrospectively removed.	low
	A parent or relative intervening in a meeting in an inappropriate way	Pupils/staff	Mod	User can be immediately be removed from the meeting or the meeting ended. If an incident occurred, the protocol would be to not engage in the conversation and either eject the parent or close the meeting down immediately.	low
	A family member accesses a pupils account via a shared device and posts/emails inappropriate content	Pupils/ staff	Low	To be covered by User Acceptance Policy Content posted in Teams can be monitored and removed. Email can be reviewed if an issue is raised.	low
	Screenshots or photographs can be taken from the video session and posted on alternative	Pupils/ staff	high	The behaviour policy is in place to extend the controls to the use of School facilities beyond the schools' premises	moderate

	social media, being made more public.				
	While sharing a document during a live recording, an alternative document containing sensitive information is shared on the video such as email	Pupils/ staff	moderate	Before starting a session, staff are required to check their desktop to ensure there are no minimised documents available that are not required during the session. Staff will follow a set checklist before starting any video session.	low